

An Enhanced Intrusion Detection System using Hybrid CNN-LSTM Architecture

Jayesh Mahawer

Sage University Indore

doi.org/10.64643/jatir.141007

Abstract—The rapid proliferation of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) has revolutionized digital infrastructure but introduced a vast attack surface for sophisticated cyber threats. Traditional Intrusion Detection Systems (IDS), which rely on signature-based matching and manual feature engineering, are increasingly fragile against zero-day exploits and polymorphic malware. This review paper examines the shift toward hybrid deep learning architectures, specifically the integration of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. By synergistically capturing both spatial intra-flow patterns and long-term temporal dependencies, these hybrid frameworks bridge the semantic gap between raw network telemetry and high-level threat identification, achieving state-of-the-art results across modern benchmark datasets.

I. INTRODUCTION

Contextualizing Industrial IoT (IIoT) Security

The Industrial Internet of Things (IIoT) represents a paradigm shift in industrial operations, facilitating large-scale device connectivity, real-time telemetry, and sophisticated automated control systems. While these advancements significantly enhance operational efficiency and device performance, they simultaneously expand the attack surface for cyber adversaries. IIoT environments are increasingly susceptible to catastrophic threats, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), ransomware, and unauthorized lateral movement within industrial control networks.

The Necessity of Advanced IDS

Traditional perimeter defenses, such as legacy firewalls and signature-based antivirus solutions, lack the granularity required to identify the polymorphic nature of modern IIoT threats. Intrusion Detection Systems (IDS) have emerged as a critical layer of defense, broadly categorized into three methodologies:

- Signature-based IDS: Exceptional at identifying known exploit patterns but inherently blind to zero-day vulnerabilities.

- Anomaly-based IDS: Employs machine learning to detect deviations from a defined "normal" baseline; however, these systems are frequently plagued by high false-positive rates in dynamic network environments.
- Hybrid IDS: Aims to synthesize the strengths of both approaches but often suffers from computational overhead and the mathematical challenges associated with manual hyperparameter configuration.

Document Overview

This research thesis presents the architecture and empirical evaluation of an optimized hybrid CNN-LSTM framework designed for IIoT security. By integrating deep learning (DL) for multi-dimensional feature extraction with Bayesian Optimization (BO) for automated model tuning, this study provides a robust, scalable defense mechanism capable of maintaining high-fidelity detection in heterogeneous industrial networks.

II. PROBLEM FORMULATION AND OBJECTIVES

Problem Statement

The deployment of effective IDS in IIoT environments is currently restricted by three fundamental bottlenecks:

1. **High False-Detection Rates:** Contemporary models often fail to distinguish between benign operational noise and malicious traffic, leading to "alert fatigue" among security analysts.
2. **Computational Inefficiency:** Many deep learning models are over-parameterized, making them unsuitable for real-time monitoring within the resource-constrained edge environments typical of IIoT.
3. **Optimization Overhead:** Conventional hyperparameter tuning methods—specifically manual grid search or heuristic-based algorithms like Particle Swarm Optimization (PSO) and Genetic Algorithms (GA)—are mathematically inefficient. These methods incur significant computational costs and often converge on local optima rather than the global maximum for model performance.

Research Objectives

This thesis establishes the following technical objectives to address the aforementioned gaps:

1. **Architectural Hybridization:** Design a "1+1" hybrid architecture consisting of a single Convolutional Neural Network (CNN) layer for spatial feature extraction and a single Long Short-Term Memory (LSTM) layer for temporal sequence modeling.
2. **Automated Hyperparameter Optimization:** Integrate a Bayesian Optimization framework to replace inefficient heuristic methods, utilizing the Tree-structured Parzen Estimator (TPE) for surrogate modeling.
3. **Cross-Dataset Validation:** Rigorously evaluate the framework across heterogeneous datasets—ToN-IoT and CICIoT2023—to ensure generalization stability.

4. **Metric Optimization:** Achieve a verifiable reduction in false alarms while maximizing detection rates and ensuring the model remains computationally feasible for edge deployment.

III. LITERATURE SURVEY

Traditional vs. AI-Based IDS

The transition from legacy Host-based (HIDS) and Network-based (NIDS) systems to Artificial Intelligence (AI) has been driven by the need for predictive rather than reactive security. Albulayhi et al. (2021) established that while traditional signature-based methods remain a baseline, they are ineffective against the rapid evolution of IoT-specific malware. Conversely, Vinayakumar et al. (2019) demonstrated that deep neural networks (DNN) possess the intrinsic capability to identify emerging attack signatures across diverse platforms, outperforming classic host-specific monitors.

Current State of Hybrid Models

The following table delineates the architectural landscape of hybrid models in recent IIoT research:

Model Architecture	Key Features	Researcher(s)	Primary Benefit
Variational LSTM	Sequential dependency focus	Zhou et al. (2021)	Enhanced anomaly detection for industrial big data
CNN-LSTM	Spatial & Temporal hybrid	Gueriani et al. (2024)	High accuracy in capturing complex traffic patterns
CNN-LSTM-Autoencoder	Unsupervised DL integration	Ain et al. (2025)	Superior mitigation of large-scale DDoS attacks
LSTM-XGBoost	DL & Gradient Boosting	Sajid et al. (2024)	Improved collaborative detection in edge nodes

Gap Analysis

Despite these advancements, the reliance on manual tuning or heuristic methods (PSO, GA) remains a critical weakness. These approaches lack the adaptive efficiency required for modern cyber-defense. Bayesian Optimization addresses this by treating the tuning process as a sequence of informed decisions, utilizing past evaluation results to sample the most promising regions of the parameter space, thereby significantly reducing the computational budget required to achieve peak model performance.

IV. PROPOSED METHODOLOGY

Methodological Workflow

The system utilizes a linear progression from data ingestion to classification, as visualized in the framework [SOURCE_IMAGE_1]:

1. Data Selection: Acquisition of high-fidelity IIoT traffic logs.
2. Preprocessing Pipeline: Formatting raw packets into model-ready tensors.
3. Model Instantiation: Construction of the hybrid CNN-LSTM layers.
4. Bayesian Tuning: Automated hyperparameter refinement.
5. Inference/Detection: Final classification of traffic as "Normal" or "Attack."

Data Preprocessing Pipeline

The pipeline ensures data quality through five distinct phases:

1. Data Cleaning: Systematic elimination of null entries and redundant records.
2. Feature Selection: Removal of non-contributory features (e.g., the 'difficulty' metric in NSL-KDD based variants) to minimize feature space dimensionality.
3. Min-Max Normalization: Rescaling all numerical input features to a standardized range of [0, 1] to ensure uniform gradient descent, utilizing the formal notation:
$$\text{X}_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$
4. One-Hot Encoding: Transformation of categorical protocol flags and service types into a machine-readable binary format.
5. Temporal Splitting: Segmenting the dataset into an 80% training partition and a 20% validation/testing partition.

Hybrid Model Architecture

As a Lead AI Architect, the priority was to design a "1+1" configuration to maximize stochastic efficiency:

- CNN Layer: A single convolutional layer extracts spatial features from the normalized input. It employs the ReLU activation function to facilitate non-linear learning and a Max-Pooling layer to down-sample feature maps while retaining high-impact spatial data.
- LSTM Layer: A single LSTM layer processes the output of the CNN to identify temporal dependencies. This layer maintains internal memory states to track sequence patterns over time. To prevent overfitting, dropout regularization is integrated into this layer.
- Output Layer: A fully connected dense layer maps the learned features to a final output. A sigmoid activation function provides the binary probability for classification.

Bayesian Optimization Framework

Hyperparameter tuning is executed via the Optuna library using the Tree-structured Parzen Estimator (TPE). TPE improves upon traditional methods by partitioning previous observations into two groups: "good" outcomes (above a performance threshold) and "bad" outcomes. It then samples the hyperparameter space by maximizing the probability of falling into the "good" group relative to the "bad." The optimization search space is defined as follows:

- CNN Filters: 32–128
- Kernel Size: 2–5
- LSTM Units: 32–128

- Dense Units: 32–128
- Dropout Rate: 0.1–0.5
- Learning Rate: 10^{-4} to 10^{-2} (log-scaled)
- Batch Size: {64, 128, 256}

V. IMPLEMENTATION

Experimental Environment

- Software: Python environment utilizing TensorFlow/Keras for model architecture and Optuna for optimization logic.
- Hardware context: The experiments were conducted on a standard laptop to simulate the compute constraints of IIoT edge environments, proving the model's viability for on-device deployment without requiring data-center-grade GPUs.

Dataset Profiles

1. ToN-IoT: Sourced from UNSW Canberra, this dataset provides a modern representation of IIoT telemetry, including actual malicious activities like reconnaissance and data exfiltration.
2. CIIoT2023: Published by the Canadian Institute for Cybersecurity, this dataset offers a highly heterogeneous environment involving diverse devices (smart TVs, webcams) to test the model's resilience against botnets and advanced persistent threats.

Baseline vs. Optimized Variants

The research compared a Baseline CNN-LSTM (standard fixed parameters) against the Proposed BO-CNN-LSTM (optimized via Bayesian logic) to quantify the specific performance lift provided by the TPE framework.

VI. RESULTS

ToN-IoT Dataset Evaluation

The optimized model demonstrated a superior ability to identify malicious patterns within the ToN-IoT telemetry. Performance gains in accuracy and discriminative power are further verified by the ROC and bar charts in [SOURCE_IMAGE_2] and [SOURCE_IMAGE_3].

Table 1: Performance Comparison on ToN-IoT Dataset

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
CNN-LSTM (Baseline)	97.98%	98.54%	97.40%	97.97%	0.9952
Proposed BO-CNN-LSTM	99.19%	99.21%	99.17%	99.19%	0.9993

The confusion matrix for the ToN-IoT evaluation [SOURCE_IMAGE_4] confirms a significant reduction in both false positives and false negatives compared to the baseline.

CIIoT2023 Dataset Evaluation

On the CICIoT2023 dataset, the model achieved near-optimal results, as evidenced by the performance metrics in [SOURCE_IMAGE_5] and the ROC curves in [SOURCE_IMAGE_6].

Table 2: Performance Comparison on CICIoT2023 Dataset | Model | Accuracy | Precision | Recall | F1-score | ROC-AUC | | :--- | :--- | :--- | :--- | :--- | :--- | | CNN-LSTM (Baseline) | 99.26% | 98.73% | 99.81% | 99.27% | 0.9972 | | Proposed BO-CNN-LSTM | 99.57% | 99.20% | 99.95% | 99.57% | 0.9991 |

The reduction in false positives on this dataset is visually detailed in the confusion matrix [SOURCE_IMAGE_7].

Key Finding Summary

- **Peak Accuracy:** 99.57% (CICIoT2023), representing a state-of-the-art result for hybrid architectures.
- **Detection Fidelity:** A recall of 99.95% ensures that almost no malicious traffic bypasses the detector.
- **Optimization Lift:** The ROC-AUC values above 0.999 across both datasets indicate near-perfect separability, validating the Bayesian approach.

VII. DISCUSSIONS

Comparative Analysis

To validate the model's competitive standing, a comprehensive comparative analysis against external benchmarks was conducted. The BO-CNN-LSTM demonstrates superior generalization stability across heterogeneous feature spaces.

Table 3: Comparative Performance Master Table (Binary Classification) | Author(s) & Year | Model Type | Dataset | Accuracy | F1-Score | | :--- | :--- | :--- | :--- | :--- | | Proposed Model (2025) | BO-CNN-LSTM | CICIoT2023 | 99.57% | 99.57% | | Proposed Model (2025) | BO-CNN-LSTM | ToN-IoT | 99.19% | 99.19% | | Yao et al. (2023) | LSTM-XGBoost | CICIoT2023 | 97.70% | 97.40% | | Gueriani et al. (2024) | CNN-LSTM | CICIoT2023 | 98.43% | 98.57% | | Abbas et al. (2024) | RNN | CICIoT2023 | 96.52% | 96.73% | | Ain et al. (2025) | CNN-LSTM+AE | CICIoT2023 | 96.78% | 96.00% | | Elghalhoud (2022) | DNN | ToN-IoT | 98.95% | 99.57% | | Elghalhoud (2022) | GBM | ToN-IoT | 98.55% | 99.18% | | Kim et al. (2020) | CNN-LSTM | CICIDS2017 | 91.93% | 86.47% |

The Impact of Bayesian Optimization

The transition from heuristic or manual tuning to Bayesian Optimization provided the "stochastic efficiency" required for high-performance IDS. By partitioning outcomes into "good" and "bad" distributions, the TPE algorithm effectively navigated the complex hyperparameter surface, avoiding the computational trap of PSO and GA methods. This resulted in a model that not only detects attacks more accurately but does so with a significantly smaller parameter footprint, making it ideal for edge implementation.

VIII. CONCLUSION AND FUTURE SCOPE

Summary of Contributions

This research successfully established a hybrid CNN-LSTM IDS architecture that leverages Bayesian Optimization to solve the persistent challenges of high false-detection rates and optimization overhead. By using a single CNN and single LSTM layer, the model achieved state-of-the-art accuracy (99.57%) while maintaining the low computational complexity required for resource-constrained IIoT environments.

Future Directions

1. Multi-class Granularity: Transition from binary "Normal vs. Attack" detection to granular classification of specific attack types (e.g., Brute Force vs. Botnet).
2. Advanced Attention Mechanisms: Integration of Transformer-based attention to better capture long-range temporal dependencies in high-speed traffic.
3. Federated Learning Integration: Implementing decentralized training protocols to allow multiple industrial sites to collaborate on security models without sharing sensitive telemetry data.
4. Hardware Testbed Validation: Moving from simulated edge environments to real-world industrial hardware (PLCs and IoT Gateways) for field validation.

REFERENCES

- [1] Abbas, S., Bouazzi, I., Ojo, S., Al Hejaili, A., Sampedro, G. A., Almadhor, A., & Gregus, M. (2024). Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. *PeerJ Computer Science*, 10, e1793. <https://doi.org/10.7717/peerj-cs.1793>
- [2] Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., & Alourani, A. (2025). Securing IoT networks against DDoS attacks: A hybrid deep learning approach. *Sensors*, 25(5), 1346.
- [3] Albulayhi, K., Smadi, A. A., Sheldon, F. T., & Abercrombie, R. K. (2021). IoT intrusion detection taxonomy, reference architecture, and analyses. *Sensors*, 21(19), 6432.
- [4] Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N. (2022). X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for Industrial Internet of Things. *IEEE Internet of Things Journal*, 9(5), 3962–3977.
- [5] Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA, and GA algorithms. *Symmetry*, 12(6), 1046.
- [6] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven Intrusion Detection Systems. *IEEE Access*, 8, 165130–165150.

- [7] Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal*, 38, 101322.
- [8] Ayyıldız, P., & Karahan, O. (2024). Hyperparameter optimization for a hybrid CNN–LSTM-based intrusion detection system. In *Cognitive Models and Artificial Intelligence Conference: SETSCI Conference Proceedings* (Vol. 17, pp. 7–12). SETSCI.
- [9] Binbusayyis, A., & Vaiyapuri, T. (2021). Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM. *Applied Intelligence*, 51(10), 7094–7108.
- [10] Elghalhoud, O. (2022). Data balancing and hyper-parameter optimization for machine learning algorithms for secure IoT networks (Master's thesis, University of Waterloo, Canada). University of Waterloo.
- [11] Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: A survey. *Journal of Cloud Computing*, 7(1), 21.
- [12] Gao, J., Chai, S., Zhang, B., & Xia, Y. (2019). Research on network intrusion detection based on incremental extreme learning machine and adaptive principal component analysis. *Energies*, 12(7), 1223.
- [13] Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Enhancing IoT security with CNN and LSTM-based intrusion detection systems. *arXiv*. <https://arxiv.org/abs/2405.18624>
- [14] Jiang, X., Lora, M., & Chattopadhyay, S. (2020). An experimental analysis of security vulnerabilities in Industrial IoT devices. *ACM Transactions on Internet Technology*, 20, 1–24.
- [15] Jose, J., & Judith, J. E. (2024). Deep Learning Model with Normalized Bayesian Optimizer for Anomaly Classification in IoT Security. *SSRG International Journal of Electronics and Communication Engineering*, 11(8), 185–199.
- [16] Kanna, P. R., & Santhi, P. (2021). Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features. *Knowledge-Based Systems*, 226, 107132.
- [17] Kasongo, S. M. (2021). An advanced intrusion detection system for IIoT based on GA and tree-based algorithms. *IEEE Access*, 9, 113199–113212.
- [18] Kheddar, H., Himeur, Y., & Awad, A. I. (2023). Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. *Journal of Network and Computer Applications*, 220, 103760.
- [19] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets, and challenges. *Cybersecurity*, 2, Article 20.
- [20] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time web intrusion detection. *IEEE Access*, 8, 70245–70261.
- [21] Makkar, A., Kim, T. W., Singh, A. K., Kang, J., & Park, J. H. (2022). SecureIIoT environment: Federated learning empowered approach for securing IIoT from data breach. *IEEE Transactions on Industrial Informatics*, 18(9), 6406–6414.

- [22] Moustafa, N. (2019). New Generations of Internet of Things Datasets for Cybersecurity Applications based Machine Learning: TON_IoT Datasets. Proceedings of the eResearch Australasia Conference, Brisbane, Australia.
- [23] Moustafa, N. (2021). TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for AI-based Cybersecurity Applications. UNSW Canberra Cybersecurity Lab.
- [24] Moustafa, N., & Slay, J. (2016). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. *Information Security Journal: A Global Perspective*, 25(1–3), 18–31.
- [25] Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIOT2023: A real-time dataset and benchmark for large-scale attacks in IoT environments. *Sensors*, 23(13), 5941. <https://doi.org/10.3390/s23135941>
- [26] Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cybersecurity in IoT networks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 452–457). IEEE.
- [27] Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. *Journal of Cloud Computing: Advances, Systems and Applications*, 13, 123.
- [28] Snoek, J., Larochelle, H., & Adams, R. P. (2012). Practical Bayesian optimization of machine learning algorithms. In F. Pereira, C. J. C. Burges, L. Bottou, & K. Q. Weinberger (Eds.), *Advances in neural information processing systems* (Vol. 25, pp. 2951–2959). Curran Associates, Inc.
- [29] Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
- [30] Xia, Z., He, S., Liu, C., Liu, Y., Yang, X., & Bu, H. (2024). PSO-GA hyperparameter optimized ResNet-BiGRU-based intrusion detection method. *IEEE Access*, 12, 135535–135550.
- [31] Yao, W., Zhao, H., & Shi, H. (2023). Privacy-preserving collaborative intrusion detection in edge of Internet of Things: A robust and efficient deep generative learning approach. *IEEE Internet of Things Journal*, 1–1.
- [32] Zhou, X., Hu, Y., Liang, W., Ma, J., & Jin, Q. (2021). Variational LSTM enhanced anomaly detection for industrial big data. *IEEE Transactions on Industrial Informatics*, 17(5), 3469–3477.