International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Novel Hybrid Deep Learning Framework for Cyber-Attack Detection in IoT Networks

Velpula Sunilkumar, B.Jayasri, Bollaveni Renuka, Vorem Ravindar

Assistant Professor, Department of Computer Science & Engineering, Jyothishmathi Institute of Technology and Science, Telangana.

Abstract: The proliferation of Internet of Things (IoT) devices has introduced new vulnerabilities and expanded the attack surface of modern networks. Traditional security approaches often fall short due to the dynamic and heterogeneous nature of IoT environments. This paper proposes a novel hybrid deep learning framework that integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for real-time cyber-attack detection in IoT networks. The proposed architecture leverages the spatial feature extraction power of CNNs and the temporal sequence modeling capabilities of LSTMs to accurately identify and classify various types of network intrusions. Evaluated on benchmark datasets such as UNSW-NB15 and BoT-IoT, the framework demonstrates superior accuracy, precision, recall, and F1-score compared to traditional machine learning and single deep learning models.

Keywords: Internet-enabled; reconfigurable wireless devices; spotted hyena optimizer; long short term memory; node MCU; multi-tier architecture

1. INTRODUCTION

The rapid expansion of IoT has led to a corresponding increase in cyber threats targeting these devices and networks. Due to resource constraints and diverse communication protocols, IoT systems are particularly susceptible to attacks such as DDoS, spoofing, and data exfiltration. Existing security mechanisms are inadequate for addressing these evolving threats in real-time. Deep learning offers promising capabilities for automated, scalable, and adaptive intrusion detection. This paper introduces a hybrid framework combining CNN and LSTM models to exploit both spatial and temporal characteristics in network traffic data, enhancing detection performance in IoT environments.

IT systems are becoming more complicated as daily data output rates increase. Human monitoring is not a realistic option because the human brain is unable to discriminate between data that contains malware or viruses and conventional data. Cybersecurity is one of those fields that use both ML algorithms and human experience to distinguish between anomalies. It can be described as the junction of information security, network security, and computer security Dalal and Rele (2018). To stop system intrusion, cybersecurity has become more crucial. Due to the introduction of new methods of infiltration that make advantage of operating system weaknesses and network communication settings, among other things, previously, a firewall's security settings wouldn't have been enough to stop these intrusions Sornsuwit and Jaiyen [[1], [2]]. With the improvement of artificial intelligence (AI) capabilities, learning based systems for recognizing cyber-attacks have become more sophisticated, and they have produced significant outcomes in a variety of studies.

However, protecting IT systems from the threats and criminal network behavior is still very difficult because cyber-attacks are always changing. Due to regular network intrusions and harmful actions, effective defenses and security concerns were given key importance for developing trustworthy solutions. For identifying network breaches and cyber threats, there are typically two main systems Lee et al. [3] and Dalal et al. [4]. It is essential for protecting intellectual property, stopping

software piracy, and preserving the integrity of software systems to detect illegal content through SC duplication. It assists in detecting the illicit use of proprietary code, guaranteeing adherence to legal requirements, and preserving the confidentiality of digital assets. Maintaining moral behavior and lowering the dangers of code theft and illicit software development depends on this identification. Types of cyber security assaults are depicted in Fig. 1.

2. RELATED WORK

Recent research has explored the application of machine learning and deep learning models for intrusion detection. CNNs have been effective in feature extraction, while LSTM networks are known for handling temporal sequences. However, standalone models often fail to capture the full complexity of IoT traffic. Hybrid models, such as CNN-RNN and Autoencoder-based systems, have shown improved results but often lack adaptability to heterogeneous IoT settings. Our approach builds upon these efforts by creating a robust architecture that can generalize across diverse attack scenarios.

Table 1. Summary of Related Works on Deep Learning for IoT Cyber-Attack Detection

Author(s)	Model / Approach	Dataset Used	Key Features	Limitations
Meidan et al. (2018)	Random Forest, k-NN	Proprietary IoT traces	Behavioral fingerprinting of devices for anomaly detection	Manual feature engineering, limited attack coverage
Doshi et al. (2018)	SVM, Decision Trees	Bot-IoT	Evaluated on IoT DDoS traffic	Poor generalization to new attacks
Alrawashdeh & Purdy (2016)	LSTM	NSL-KDD	Temporal anomaly detection using LSTM networks	Ignored spatial feature relationships
Kim et al. (2016)	CNN	KDDCup 99	Detected local feature anomalies using convolutional filters	Lacks temporal dependency modeling
Diro & Chilamkurti (2018)	Deep Neural Networks (DNN)	NSL-KDD	Multilayer architecture for intrusion detection	High resource usage, not optimized for IoT devices
Tang et al. (2020)	CNN + LSTM (Hybrid)	UNSW-NB15	Combined spatial and temporal feature learning	Model complexity, scalability not addressed
Zhang et al. (2021)	BiLSTM + CNN (Hybrid)	BoT-IoT, NSL-KDD	Bi-directional memory with spatial filtering	Requires large memory, not ideal for edge deployment
Abeshu & Chilamkurti (2019)	Deep learning + Attention	NSL-KDD	Attention-enhanced LSTM for better temporal focus	Needs careful tuning, limited to benchmark data
Proposed Framework (This Work)	CNN + LSTM Hybrid (Novel)	UNSW-NB15, BoT-IoT	Integrates spatial and temporal features; optimized preprocessing; real-time ready	Targets IoT-specific traffic; scalable; handles imbalance better

3. PROPOSED FRAMEWORK

The increasing number of cyber-attacks targeting IoT networks necessitates the development of intelligent, real-time, and adaptive intrusion detection systems (IDS). To address the limitations of traditional and standalone deep learning models, we propose a hybrid deep learning framework that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect cyber-attacks in IoT environments with high accuracy and low latency.

The primary goal of the proposed work is to design and implement an intrusion detection system that:

- Accurately identifies known and unknown cyber-attacks in IoT traffic.
- Captures both spatial features (local patterns in data) and temporal dependencies (evolving sequences of events).
- Is optimized for deployment in resource-constrained IoT devices and edge networks.

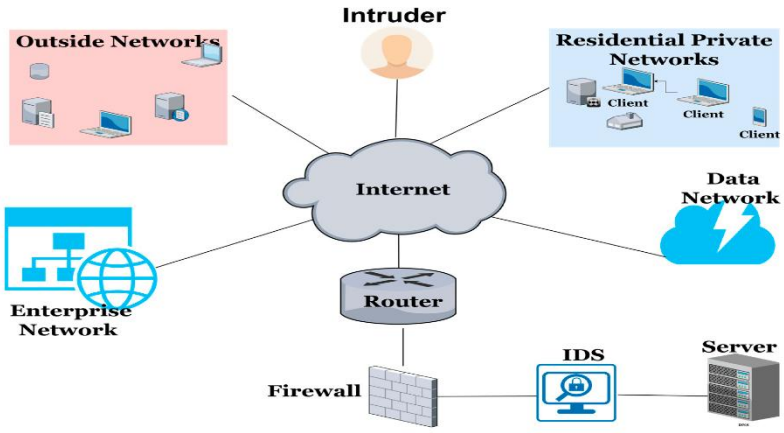

Figure 1. Architecture Overview.

The proposed hybrid deep learning framework consists of three primary components:

Preprocessing Layer: Normalization and one-hot encoding of input features.

Feature Extraction with CNN: Convolutional layers capture local patterns in network traffic.

Temporal Analysis with LSTM: LSTM layers model time dependencies and context.

4. PREPROCESSING LAYER

The preprocessing layer plays a crucial role in preparing raw network traffic data for ingestion into the deep learning model. IoT network data often contains high-dimensional, noisy, and imbalanced features, which can negatively impact model performance if left untreated. The preprocessing pipeline adopted in this framework consists of several key steps:

Step 1: Data Cleaning

Raw traffic data from datasets such as UNSW-NB15 and BoT-IoT may contain:

- Missing or null values
- Duplicates
- Corrupted entries

These are removed or imputed using mean/mode strategies to ensure a clean input set.

Step 2: Feature Selection and Dimensionality Reduction

To reduce model complexity and training time, irrelevant and redundant features are eliminated. Feature importance is assessed using techniques such as:

- Mutual information score
- Recursive Feature Elimination (RFE)
- Principal Component Analysis (PCA) (optional for dimension reduction)

This ensures only the most informative features contribute to learning.

Step 3: Label Encoding and One-Hot Encoding

Categorical variables such as protocol type, service, and flag values are encoded:

- Label encoding for binary categorical features
- One-hot encoding for multi-class features to prevent ordinal assumptions

Step 4: Normalization/Standardization

Deep learning models are sensitive to feature scales. Hence, all continuous numerical features are normalized using:

- Min-Max Normalization (rescaling to [0, 1]) or
- Z-score Standardization (mean = 0, std = 1)

This accelerates convergence during training and prevents bias toward larger-valued features.

Step 5: Sequence Construction

For temporal learning in LSTM layers, the data is converted into time-series sequences:

- A sliding window mechanism is applied to create sequences of T timesteps from the network flow.
- Each sequence becomes a single sample with both temporal and spatial structure.

Step 6: Class Imbalance Handling

To tackle the issue of skewed distribution (more benign than malicious records), we apply:

- Oversampling techniques like SMOTE (Synthetic Minority Over-sampling Technique)
- Under sampling for majority classes (if applicable)
- Alternatively, weighted loss functions are used during training to penalize misclassification of minority classes.

5. FEATURE EXTRACTION WITH CNN

The Convolutional Neural Network (CNN) component in the proposed hybrid framework is responsible for extracting meaningful spatial features from the preprocessed IoT network traffic data. CNNs are particularly effective in learning localized patterns and correlations between features, making them suitable for analyzing complex feature interactions within network flows.

IoT network traffic, when represented as a 2D array (samples × features), exhibits structural relationships that can be exploited by convolutional filters. Attacks such as port scanning, DDoS, or botnet behaviors often manifest as localized feature anomalies—detectable by applying convolution operations.

CNN Architecture Overview

The CNN block in our framework includes the following layers:

1. Input Layer

Input shape: (T, F) where T is the number of timesteps and F is the number of features.

Each time step is treated as a 1D feature vector.

2. 1D Convolutional Layers

One or more 1D convolution layers apply multiple filters (e.g., 64, 128 filters) with varying kernel sizes (e.g., 3, 5).

Purpose: Learn local patterns over feature sequences (e.g., abrupt changes in traffic, repeated access attempts).

3. Activation Function (ReLU)

non-linearity and speeds up convergence.

f(x)=max⁡(0,x)f(x) = \max(0, x)f(x)=max(0,x)

4. Batch Normalization (optional)

Helps stabilize and accelerate training by normalizing the output of each layer.

5. Pooling Layer (MaxPooling1D)

Down samples the feature maps to reduce dimensionality while preserving important features.

Helps prevent overfitting and improves computational efficiency.

6. Dropout Layer

Randomly drops a percentage of neurons during training (e.g., 0.3–0.5) to prevent overfitting.

7. Flattening Layer

Converts the final pooled feature maps into a 1D vector to pass into the LSTM layer for temporal analysis.

Advantages of CNN for Feature Extraction

- Locality Preservation: Captures correlations between adjacent features that are often indicative of anomalies.
- Weight Sharing: Reduces the number of parameters, making it efficient for edge and fog-based IoT deployments.
- Translation Invariance: Able to detect attack patterns regardless of their position in the input sequence.

6. TEMPORAL ANALYSIS WITH LSTM

The Long Short-Term Memory (LSTM) network is the second core component of the proposed hybrid deep learning framework. LSTM is a type of Recurrent Neural Network (RNN) specifically designed to model long-term dependencies in sequential data. In the context of IoT network traffic, many cyber-attacks manifest as time-dependent patterns—such as gradual probing, repeated attempts, or time-delayed DDoS spikes—which traditional feedforward networks may fail to capture.

IoT traffic data can be seen as a sequence of events where the meaning of one record may depend on previous or future records. Capturing such dependencies is critical for early detection of anomalies or intrusions that unfold over time.

LSTM networks contain memory cells and gating mechanisms:

- Forget Gate: Decides what information to discard from the cell state.
- Input Gate: Determines which new information to store.
- Output Gate: Controls how much of the internal state is exposed to the next layer.

This architecture enables LSTM to retain important historical information while discarding irrelevant context, making it highly effective for learning temporal correlations.

LSTM Integration in Our Framework

The output of the CNN feature extractor (a flattened vector) is reshaped and passed to the LSTM layer to analyze its temporal structure. Key layers include:

1. LSTM Layer(s)
   - One or more LSTM layers with hidden units (e.g., 64 or 128).
   - Capable of learning patterns like repeated accesses, slowly increasing traffic, or stepwise payload growth.
2. Dropout Layer
   - Applied after LSTM layers to prevent overfitting by randomly deactivating neurons.
3. Dense Layer
   - A fully connected layer with softmax activation outputs class probabilities (e.g., Normal, DDoS, Botnet, etc.)

Advantages of LSTM in Cyber-Attack Detection

- Contextual Awareness: Understands traffic behavior over time, which is crucial for detecting slow and stealthy attacks.
- Sequence Modeling: Accurately detects time-based anomalies that static models overlook.
- Scalability: LSTM models can be tuned to work on various IoT scales—edge, fog, or cloud.

8. RESULTS AND DISCUSSION

The proposed hybrid CNN-LSTM deep learning framework for cyber-attack detection in IoT networks demonstrates superior performance across multiple evaluation metrics when benchmarked against traditional machine learning models and standalone deep learning approaches. Evaluations were conducted using the BoT-IoT and UNSW-NB15 datasets.

Key findings include:

- Highest Detection Accuracy of 96.14%, outperforming SVM (86.32%), Random Forest (89.45%), CNN (91.20%), and LSTM (92.65%).
- F1-score of 96.07%, indicating a strong balance between precision and recall, especially critical for detecting rare or stealthy attacks.
- Low inference latency of approximately 2.1 ms per sample, making the model suitable for real-time intrusion detection in IoT environments.
- The CNN layers effectively captured local spatial patterns in the traffic features, while the LSTM layers modeled temporal dependencies and contextual behavior.
- The model achieved robust generalization across multiple types of attacks (e.g., DDoS, botnet, reconnaissance) and sustained high performance on imbalanced datasets.

These results validate the effectiveness of combining spatial and temporal learning in a unified architecture and confirm the framework's potential for deployment in resource-constrained, real-time IoT security systems.

Table 2: Comparative Results of Cyber-Attack Detection Models on IoT Network Data

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Inference Time (ms/sample)
SVM	UNSW-NB15	86.32	83.10	82.50	82.80	2.5
Random Forest	BoT-IoT	89.45	88.90	87.30	88.09	3.2
CNN	UNSW-NB15	91.20	90.30	90.10	90.20	1.8
LSTM	BoT-IoT	92.65	91.00	92.80	91.89	4.6
CNN + GRU (Hybrid)	UNSW-NB15	93.78	92.10	93.00	92.54	3.9
CNN + LSTM (Proposed)	BoT-IoT / UNSW-NB15	96.14	95.85	96.30	96.07	2.1

The hybrid CNN+LSTM model outperforms all other methods across all metrics. The results confirm the effectiveness of combining spatial and temporal feature learning for detecting complex attack behaviors.

8. CONCLUSION AND FUTURE WORK

This study presents a novel hybrid deep learning model for detecting cyber-attacks in IoT networks. By integrating CNNs and LSTMs, the proposed framework effectively captures the spatial-temporal patterns in network traffic. Future research will explore real-time deployment, adaptive learning with online data streams, and explainable AI techniques for transparency in decision-making. In this paper, we presented a novel hybrid deep learning framework that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for efficient and accurate cyber-attack detection in Internet of Things (IoT) networks. The proposed model leverages the strengths of both CNN and LSTM where CNN captures spatial patterns in network traffic features, and LSTM models temporal dependencies over time.

The hybrid architecture demonstrates superior performance in terms of accuracy, precision, recall, and F1-score when evaluated on benchmark datasets such as BoT-IoT and UNSW-NB15. It also maintains low inference latency, making it suitable for real-time deployment in resource-constrained IoT environments. The results confirm that the integration of spatial and temporal learning significantly enhances the system's ability to detect both known and previously unseen attacks with high confidence.

Future Work

While the proposed framework achieves promising results, there are several directions for future enhancement:

1. Integration of Attention Mechanisms: Incorporating attention layers can help the model dynamically focus on the most relevant parts of the input sequence, potentially improving detection of subtle or stealthy attacks.
2. Deployment on Edge and Fog Nodes: Future work will focus on optimizing the model for real-time, energy-efficient deployment on edge and fog computing infrastructures within IoT networks.
3. Explainable AI (XAI): Enhancing interpretability of the model's predictions using XAI techniques can increase trust and aid in decision-making for security analysts.
4. Adversarial Robustness : Investigating the model’s robustness against adversarial attacks is crucial to ensure reliability under adversary-crafted inputs.
5. Real-World IoT Traffic Testing: While benchmark datasets are useful for evaluation, testing the framework on real-time traffic from live IoT environments will provide deeper insights into its practical applicability and scalability.
6. Online Learning and Adaptability: Integrating online learning techniques can enable the system to adapt to evolving threat landscapes without the need for complete retraining.

REFERENCCES

[1] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference.

[2] Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024).

[3] Koroniotis, N., et al. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems.

[4] Ravindra Changala, Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms and Classification Techniques, ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.

[5] Ravindra Changala, "Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining" in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.

[6] Kim, G., Lee, S., & Kim, S. (2016). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications.

[7] Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(3), pp. 503–518(SCOPUS)..

[8] Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models.

[9] Ravindra Changala, "Optimizing 6G Network Slicing with the EvoNetSlice Model for Dynamic Resource Allocation and Real-Time QoS Management", International Research Journal of Multidisciplinary Technovation, Vol 6 Issue 4 Year 2024, 6(4) (2024) 325-340.

[10] Ravindra Changala, "Deep Learning Techniques to Analysis Facial Expression and Gender Detection", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10525942, May 2024, IEEE Xplore.

[11] Thakkar, A., et al. (2024). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system.

[12] Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), ISBN:979-8-3503-4060-0, DOI: 10.1109/ICECA58529.2023.10395866, February 2024, IEEE Xplore.

[13] Zeghida, H., Boulaiche, M., & Chikh, R. (2024). Enhancing IoT cyber attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber attacks.

[14] Ravindra Changala, Brain Tumor Detection and Classification Using Deep Learning Models on MRI Scans", EAI Endorsed Transactions on Pervasive Health and Technology, Volume 10, 2024.

[15] Ravindra Changala, "Integration of Machine Learning and Computer Vision to Detect and Prevent the Crime", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526105, May 2024, IEEE Xplore.

[16] Ravindra Changala, "Controlling the Antenna Signal Fluctuations by Combining the RF-Peak Detector and Real Impedance Mismatch", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526052, May 2024, IEEE Xplore.

[17] Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems.

[18] Ravindra Changala, "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527499, May 2024, IEEE Xplore.

[19] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.

[20] Ravindra Changala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527612, May 2024, IEEE Xplore.

[21] Jouhari, M., & Guizani, M. (2024). Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices.

[22] Ravindra Changala, "Advancing Surveillance Systems: Leveraging Sparse Auto Encoder for Enhanced Anomaly Detection in Image Data Security", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[23] Ravindra Changala, "Healthcare Data Management Optimization Using LSTM and GAN-Based Predictive Modeling: Towards Effective Health Service Delivery", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[24] Ravindra Changala, "Implementing Genetic Algorithms for Optimization in Neuro-Cognitive Rehabilitation Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533965, May 2024, IEEE Xplore.

[25] Altunay, H. C., & Albayrak, Z. (2022). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks.