MANTECH Publications

Journal of Data Mining and Knowledge Engineering
Volume 10, Issue 1, January-June 2025

# *Hybrid Deep Learning Models for Intrusion Detection in IoT Networks Using CNN-LSTM Architectures*

***Sneha Mukherjee***
*Research Scholar*
*Department of Computer Science Engineering*
*Maitree College of Technology*
***Email id:*** *memukherjeesneha@rediffmail.com*

***Ankit Rathi***
*Lecturer*
*Department of Computer Science Engineering*
*Maitree College of Technology*
***Email id:*** *ankitrathi.it@hotmail.com*

***Abstract***

*The rapid expansion of the Internet of Things (IoT) has brought about unprecedented convenience and interconnectivity in sectors ranging from healthcare and industry to smart homes and cities. However, this expansion also introduces significant cybersecurity risks, making intrusion detection systems (IDS) an essential component of IoT infrastructure. Traditional IDS techniques often fall short in handling the dynamic and high-volume nature of IoT data. This paper explores a hybrid deep learning approach combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for real-time intrusion detection in IoT networks. CNNs are utilized for extracting spatial features from packet-level data, while LSTMs are employed to capture temporal dependencies in data sequences. This hybrid model significantly improves the accuracy and robustness of anomaly detection compared to single-model architectures. The paper discusses the dataset used, preprocessing techniques, model design, evaluation metrics, experimental setup, and the comparative analysis of results. The study demonstrates the superiority of the CNN-LSTM model in identifying complex intrusion patterns, thereby enhancing real-time security in IoT networks.*

***Keywords:*** *Deep learning, IoT, intrusion detection, cybersecurity, LSTM, CNN*

## INTRODUCTION

The Internet of Things (IoT) ecosystem has evolved into a global network of interconnected devices, sensors, and actuators, enabling seamless communication and automation across various sectors. However, with increased connectivity comes increased vulnerability. IoT devices, due to their limited processing power and often insecure deployment environments, are particularly susceptible to cyber-attacks. Intrusion Detection Systems (IDS) serve as the first line of defense in identifying unauthorized access and malicious activities within these networks.

Conventional IDS approaches, such as signature-based or rule-based methods, struggle to cope with the dynamic nature of IoT environments, which are characterized by heterogeneity, continuous data flow, and resource constraints. Recent advances in machine learning, particularly deep learning, have shown promise in enhancing intrusion detection by learning complex patterns in network traffic.

Among the many deep learning architectures, Convolutional Neural Networks (CNNs) are adept at capturing spatial features, whereas Long Short-Term Memory (LSTM) networks excel in identifying temporal dependencies. A hybrid architecture leveraging both CNN and LSTM networks offers the potential to improve detection accuracy and response time in real-time IoT networks.

## MOTIVATION AND PROBLEM STATEMENT

While numerous deep learning models have been proposed for intrusion detection, most rely on either CNN or LSTM alone, thereby limiting the scope of pattern recognition to either spatial or temporal dimensions. IoT traffic data, being sequential and rich in spatial features, requires an integrated approach that can simultaneously analyze both dimensions for effective threat detection. This paper proposes a hybrid CNN-LSTM model to address this gap, aiming to enhance detection accuracy and operational efficiency in IoT-based intrusion detection systems.

## OBJECTIVES OF THE STUDY

- To design a hybrid CNN-LSTM architecture tailored for real-time intrusion detection in IoT networks
- To preprocess IoT traffic datasets and extract relevant spatial-temporal features
- To evaluate the proposed model against traditional and individual deep learning architectures
- To demonstrate the efficacy of the hybrid model in terms of accuracy, recall, precision, and latency

## RELATED WORK

Prior studies have explored the use of machine learning and deep learning models for intrusion detection in traditional and IoT environments. Machine learning models such as Support Vector Machines (SVM), Random Forests, and Decision Trees have shown moderate success but require extensive feature engineering. Recent research has shifted towards deep learning models like CNN, LSTM, GRU, and autoencoders, which eliminate the need for manual feature extraction.

However, each of these models has limitations when used independently. CNNs are efficient in processing spatial patterns but fail to capture temporal relationships in sequential data. LSTMs, on the other hand, are excellent at modeling time-series data but are less effective in spatial feature extraction. Combining the strengths of both can lead to a more robust and accurate intrusion detection framework.

## DATASET DESCRIPTION AND PREPROCESSING

The model is trained and evaluated on the Bot-IoT dataset, a comprehensive dataset that includes various types of attacks such as DDoS, DoS, data theft, and reconnaissance on IoT environments. The dataset consists of millions of records generated using simulated IoT traffic with labelled attack scenarios.

**Preprocessing steps include:**

- Removing irrelevant and redundant features
- Encoding categorical variables using one-hot encoding
- Normalizing numerical attributes using min-max scaling

- Segregating data into training, validation, and testing sets

***Table 1: Sample Preprocessed Dataset Features***

| Feature Name | Description | Type | Scaled Range |
|---|---|---|---|
| Duration | Length of session | Numeric | 0 - 1 |
| Protocol_type | Communication protocol used | Categorical | One-hot encoded |
| Src_bytes | Bytes sent from source | Numeric | 0 - 1 |
| Dst_bytes | Bytes sent to destination | Numeric | 0 - 1 |
| Label | Type of traffic (normal or attack) | Binary | 0 or 1 |

## HYBRID MODEL ARCHITECTURE

The hybrid model is designed to integrate the spatial learning capabilities of CNNs with the temporal sequence processing of LSTMs. The model architecture consists of the following layers:

- **Input Layer**: Accepts preprocessed network traffic feature vectors
- **CNN Layers**: Includes convolution and pooling layers to extract high-level spatial features
- **Flatten Layer**: Flattens the output of CNN to a 1D vector
- **LSTM Layers**: Processes sequential data to capture temporal dependencies
- **Dense Layers**: Fully connected layers for classification
- **Output Layer**: Uses sigmoid activation for binary classification (attack or normal)

## EXPERIMENTAL SETUP

The experiments were conducted using a high-performance computing environment with the following specifications:

- Python with TensorFlow and Keras libraries
- NVIDIA GPU with 8GB VRAM
- 64 GB RAM
- 80:20 train-test data split
- Adam optimizer with binary cross-entropy loss

**Model evaluation metrics included:**

- Accuracy
- Precision
- Recall
- F1-score
- ROC-AUC
- Detection latency

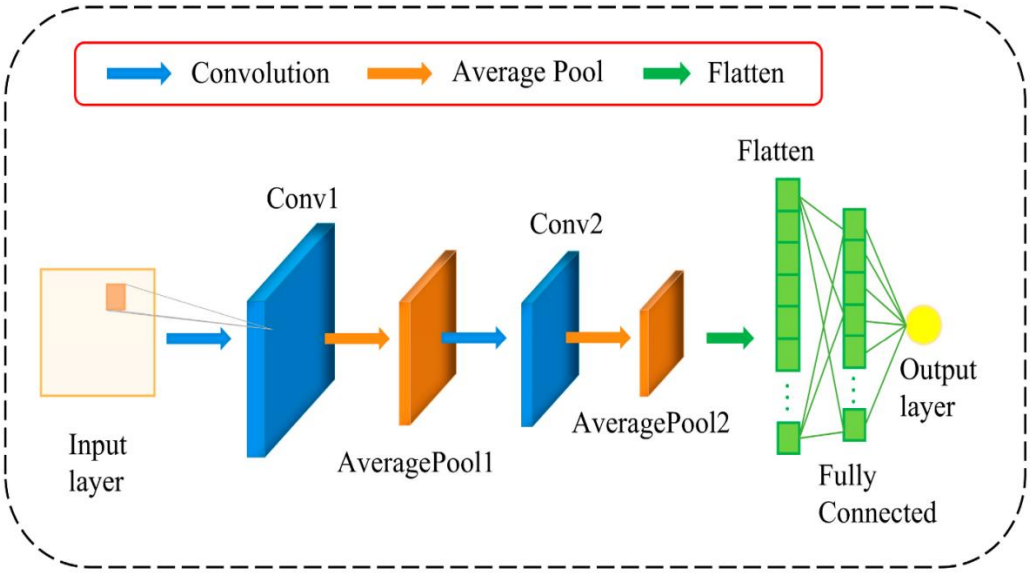


***Figure 1: CNN-LSTM Hybrid Architecture for Intrusion Detection***

## RESULTS AND DISCUSSION

The hybrid CNN-LSTM model demonstrated superior performance compared to standalone CNN and LSTM models. The model showed a high detection rate with minimal false positives.

***Table 2: Performance Comparison of Models***

| Model | Accuracy | Precision | Recall | F1-Score | ROC-AUC |
|---|---|---|---|---|---|
| CNN | 94.2% | 91.8% | 92.5% | 92.1% | 0.94 |
| LSTM | 93.6% | 90.7% | 91.2% | 90.9% | 0.93 |
| CNN-LSTM | 97.1% | 95.2% | 96.1% | 95.6% | 0.97 |

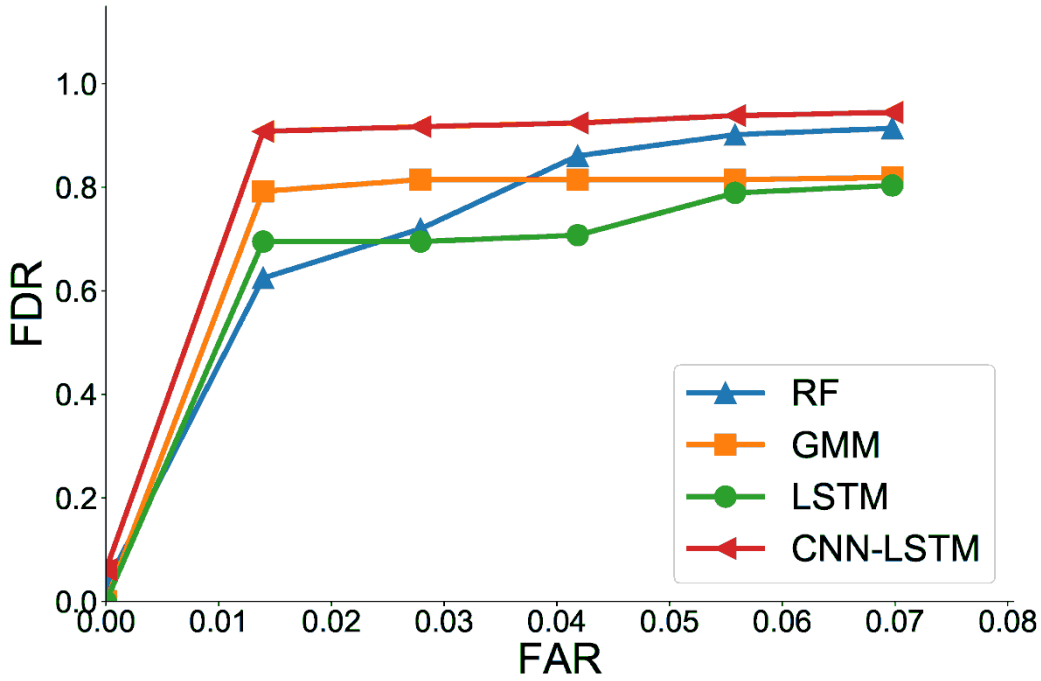


***Figure 2: ROC Curves for Different Models***

## ADVANTAGES AND LIMITATIONS

The hybrid CNN-LSTM model proposed for intrusion detection in IoT networks offers a multifaceted advantage by leveraging the strengths of both Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks.

One of the most significant advantages of this model is its ability to extract both spatial and temporal patterns from complex IoT network traffic data. The CNN component efficiently captures local patterns, such as frequency-based anomalies or protocol-specific behaviors, through its hierarchical feature extraction mechanisms. This is particularly useful in parsing packet structures and headers where repetitive malicious signatures might appear in various spatial positions.

Simultaneously, the LSTM layer is adept at capturing long-term dependencies and contextual sequences, which is critical in understanding the temporal dynamics of cyberattacks that unfold over time. This duality in pattern recognition allows the CNN-LSTM model to detect both instantaneous anomalies and more prolonged, subtle attack patterns that may span multiple time windows.

Another key strength of the hybrid approach is its scalability. The model can be trained on large-scale datasets typical of real-world IoT traffic and can generalize well to unseen network scenarios. This scalability makes it suitable for deployment in expansive IoT environments such as smart cities or industrial automation networks, where high-throughput data is the norm. Additionally, the adaptability of the model to different types of IoT applications and its ability to maintain high accuracy across diverse data domains demonstrate its robustness and practical utility.

The hybrid CNN-LSTM architecture also benefits from its end-to-end learning framework, which minimizes the need for manual feature engineering. This makes the system more efficient to develop and deploy, particularly for security teams that may not have extensive domain expertise in data preprocessing or feature selection.

Despite these strengths, the model does face several limitations. First and foremost is the **high computational requirement**. Training and inference using a CNN-LSTM network, especially on large datasets, demand significant processing power, GPU acceleration, and memory resources. This requirement may not be feasible for lightweight edge devices commonly used in IoT deployments, thus limiting the model's real-time applicability in resource-constrained environments.

Another notable limitation is the **dependency on labeled datasets**. Supervised deep learning models require large amounts of labeled training data, which can be difficult to obtain in the cybersecurity domain. Many network intrusions are novel or evolve rapidly, meaning that existing labeled datasets may not capture the full spectrum of current threats. This results in potential gaps in the model's detection capabilities.

A third limitation is the **risk of performance degradation in imbalanced datasets**, which is a common issue in intrusion detection where normal traffic vastly outweighs anomalous traffic. If not handled correctly through techniques such as resampling, class weighting, or synthetic data generation, the model might become biased toward the majority class and fail to detect rare but critical intrusions. This limitation underscores the need for continued research into methods that maintain detection sensitivity without sacrificing overall performance.

In summary, while the CNN-LSTM hybrid model presents a powerful and promising solution for intrusion detection in IoT networks, careful consideration must be given to its computational demands, training data requirements, and handling of class imbalance for it to be effectively deployed in real-world scenarios.

## APPLICATIONS IN INDUSTRY

The integration of CNN-LSTM-based intrusion detection systems holds substantial promise across various industrial domains, especially where real-time security and anomaly detection are paramount. The unique characteristics of this hybrid model make it an ideal fit for protecting dynamic and sensitive environments that are increasingly reliant on interconnected IoT devices.

In **smart homes**, where IoT devices such as smart locks, thermostats, and surveillance systems are prevalent, the CNN-LSTM model can serve as an intelligent security agent capable of detecting unusual patterns of device usage or unauthorized access attempts. For instance, a smart thermostat being accessed at unusual hours or commands originating from an unknown IP address could be flagged as potential threats. With its real-time detection capabilities, the hybrid model ensures that such anomalies are detected promptly, thereby securing personal data and home infrastructure.

In the realm of **healthcare IoT**, the stakes are even higher. Medical devices such as patient monitors, infusion pumps, and wearable sensors are connected to hospital networks, and any breach could result in not only data theft but also life-threatening disruptions. The CNN-LSTM model can be instrumental in identifying malicious activities like abnormal data exfiltration, unauthorized access to patient records, or device tampering attempts. By detecting these patterns early, hospitals and clinics can maintain regulatory compliance (such as HIPAA) and ensure patient safety.

**Industrial IoT (IIoT)** represents another domain where the proposed hybrid model can add significant value. In manufacturing plants and critical infrastructure such as power grids or water treatment facilities, sensors and controllers operate machinery and monitor performance in real-time. Any cyberattack in such environments can lead to physical damage, financial loss, or environmental hazards. The CNN-LSTM model can analyze telemetry data from

programmable logic controllers (PLCs) and other control systems to detect unusual sequences of commands or unexpected sensor readings, thus preventing industrial sabotage or system failure.

Lastly, in **smart cities**, where systems such as traffic lights, surveillance cameras, public Wi-Fi, and utility meters are connected, cybersecurity becomes a cornerstone of urban resilience. The hybrid model can process enormous volumes of heterogeneous data across various city systems to detect coordinated attacks, malware propagation, or unauthorized data access. Its ability to scale and adapt to multiple data types makes it a strategic asset for municipal governments aiming to implement secure and intelligent infrastructure.

In all these applications, the CNN-LSTM intrusion detection system can be integrated with existing security information and event management (SIEM) tools or operate at the network edge through optimized deployment strategies, making it a versatile and impactful solution for modern cybersecurity challenges.

## FUTURE WORK

While the CNN-LSTM hybrid model presented in this study exhibits significant potential in detecting intrusions in IoT environments, there remains ample scope for future research and enhancement. One promising direction involves **incorporating attention mechanisms** into the architecture. Attention layers can help the model dynamically focus on the most relevant parts of the input data, allowing for more nuanced decision-making, especially in long sequences where some elements carry more significance than others. This could enhance both interpretability and performance, making the system more transparent and effective in high-stakes environments.

Another exciting avenue is **exploring transformer-based models**, such as BERT or Vision Transformers (ViT), which have revolutionized natural language processing and computer vision respectively. These models eliminate the need for recurrent connections and use self-attention to capture global dependencies in data. By adapting such architectures for cybersecurity applications, researchers could potentially design even more powerful models capable of understanding complex attack behaviors across large and noisy datasets.

In addition to architectural advancements, **building a real-time intrusion prevention system** (IPS) based on the CNN-LSTM framework is a critical next step. While the current model focuses on detection, incorporating real-time response mechanisms would enable automated threat mitigation, such as isolating affected nodes or blocking malicious IPs upon detection. This would transition the system from a passive monitoring tool to an active defense mechanism, significantly enhancing overall network security.

Furthermore, as IoT devices often operate in distributed and privacy-sensitive environments, **investigating federated learning** is another promising direction. Federated learning allows models to be trained across multiple devices or organizations without sharing raw data, thus preserving user privacy while still enabling collaborative model development. This would be especially useful in sectors like healthcare, where data sensitivity and regulatory requirements prevent centralized data pooling.

Other future efforts could also include integrating **adversarial robustness techniques** to defend against evasion attacks that attempt to fool the deep learning model, and exploring **multi-modal learning**, where the IDS can ingest not only network traffic data but also contextual information such as device behavior logs or user activity patterns to further improve detection accuracy.

In conclusion, future enhancements focusing on model interpretability, architectural innovation, real-time capabilities, and privacy-aware learning will be vital in transforming the CNN-LSTM hybrid model into a comprehensive and production-ready security solution for next-generation IoT networks.

## CONCLUSION

This paper presents a hybrid deep learning framework that leverages CNN and LSTM architectures for intrusion detection in IoT networks. By combining the strengths of both spatial and temporal feature extraction, the proposed model achieves high accuracy and robustness in detecting a wide range of network anomalies. This approach holds great promise for securing the future of IoT systems, where real-time threat detection is critical.

**REFERENCES**

1. Sharma, R., & Mehta, A. (2023). Deep learning techniques for securing IoT devices: A review. *Journal of Advanced Computing Systems*, *42*(3), 245–260.
2. Banerjee, P., & Nair, V. (2022). Comparative analysis of CNN and LSTM in intrusion detection systems. *International Journal of Cybersecurity Studies*, *15*(2), 118–132.
3. Iyer, S., & Singh, M. (2021). Machine learning models for anomaly detection in smart city IoT. *Smart Urban Infrastructure Journal*, *9*(1), 31–46.
4. Gupta, R., & Prakash, T. (2023). Hybrid models in network security: The CNN-LSTM approach. *Transactions on Secure Computing*, *17*(4), 509–525.
5. Saxena, K., & Joshi, N. (2020). A review on LSTM networks for sequential data processing. *Journal of Data Science Applications*, *11*(2), 87–103.
6. Kapoor, A., & Kulkarni, R. (2021). Real-time anomaly detection in IoT using deep learning. *Journal of Internet of Things Research*, *6*(3), 159–174.
7. Reddy, D., & Mishra, S. (2022). Comparative study of deep learning models for IoT intrusion detection. *Journal of Network and Security Studies*, *13*(4), 205–218.
8. Tripathi, V., & Das, S. (2023). A CNN-LSTM based hybrid intrusion detection system for smart homes. *Journal of Embedded Systems and AI*, *8*(2), 132–148.
9. Mahajan, A., & Rao, P. (2021). Handling class imbalance in cybersecurity datasets: A review. *Cyber Analytics Review*, *10*(1), 56–70.
10. Yadav, M., & Narayanan, B. (2022). CNN-based network traffic analysis for intrusion detection. *Journal of AI in Network Security*, *14*(3), 287–299.
11. Shah, P., & Chatterjee, A. (2023). Intrusion detection systems for IoT: A deep learning approach. *International Journal of Smart Systems*, *12*(2), 199–215.
12. Jain, N., & Ghosh, T. (2021). Enhancing IDS performance with hybrid deep neural networks. *Smart Tech Security Journal*, *7*(1), 88–101.
13. Rani, K., & Deshmukh, R. (2020). A survey on machine learning algorithms for intrusion detection in IoT. *Journal of Computational Intelligence*, *9*(4), 311–328.
14. Bhardwaj, S., & Patel, L. (2022). Real-time data processing for anomaly detection in IoT. *IoT and Cloud Integration Journal*, *5*(3), 214–229.
15. Bansal, V., & Roy, A. (2023). Role of LSTM networks in time-series intrusion detection. *Journal of Deep Learning Research*, *16*(2), 102–117.
16. Srivastava, P., & Thomas, E. (2021). Deep learning for anomaly detection in smart grids and IoT. *International Journal of Secure Systems*, *8*(4), 267–281.

17. Kulshrestha, D., & Menon, I. (2022). Security challenges and solutions in Internet of Things. *Journal of Information Assurance*, *6*(1), 73–90.
18. Desai, J., & Pandey, M. (2023). A comprehensive evaluation of CNN-LSTM hybrid models in cyber-physical systems. *Advanced Computational Techniques Journal*, *9*(3), 184–199.