Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1983–1994
DOI : 10.47974/JIOS-2027

Hybrid deep learning-based IoT intrusion detection : A comparative study of CNN, GRU, LSTM, and hybrid architectures

Sonkarlay J.Y. Weamie [*]
College of Computer Science and Electronic Engineering
Hunan University
Yuelu District
Changsha 410082
Hunan
China

Vinothkumar Kolluru [†]
Department of Data Science
Stevens Institute of Technology
1 Castle Point Terrace
Hoboken 07030
NJ
U.S.A.

AB Jallah Balyemah [§]
College of Computer Science and Electronic Engineering
Hunan University
Yuelu District
Changsha 410082
Hunan
China

[*] *ORCID-ID:* 0000-0002-9414-7171
[†] *ORCID-ID:* 0009-0006-1713-5720
[§] *ORCID-ID:* 0009-0002-8815-6060

[*] *E-mail:* skweamie@hnu.edu.cn (Corresponding Author)
[†] *E-mail:* vkolluru@stevens.edu
[§] *E-mail:* ab.jallah1990@gmail.com

Yagnesh Challagundla [‡]
Department of Engineering Education
Herbert Wertheim College of Engineering
University of Florida
Gainesville 32611
Florida
U.S.A.

Abstract

Cyber-physical systems, particularly Internet of Things devices, pose significant cybersecurity challenges due to their vast volume, speed, and complexity of network traffic and attack vectors. This research presents an innovative hybrid deep learning technique to improve intrusion detection by taking full advantage of spatial and temporal characteristics from IoT network traffic. In this paper, we conduct a systematic study to compare different deep learning models, including CNN, GRUs, and LSTM networks, as well as their hybrid architectures such as CNN- GRU and CNN-LSTM on real-world NB-IoT dataset with benign traffic traces mixed up against targeted attacks from Mirai/Gafgyt botnets. The CNN-LSTM hybrid model demonstrated significant performance in IoT intrusion detection, achieving accuracy rates of 94.7%, precision of 94.6%, recall of 94.7%, and F1-score of 94.6%.

Subject Classification: *68T07, 68T45, 68M10.*

Keywords: *CNN-LSTM, CNN-GRU, Deep learning, Hybrid models, GRU-CNN, IoT security, IDS.*

1. Introduction

The expansion of the Internet of Things has caused several sectors to undergo profound transformations. With advanced automation and connectivity, data-driven insights given across this domain are becoming routine and invaluable for business decision-making purposes. However, the increase in IoT-connected devices has significantly widened the potential targets for cyber-attacks, leading to a rise in such attacks on these devices [1]. The diverse and resource-constrained nature of IoT environments, including smart home appliances, healthcare sensors, and industrial IoT devices, makes it difficult for IDS models to distinguish between legitimate and illegal traffic [2]. Traditional IDS are no longer effective in these modern, integrated, and complex environments because they are unable to identify new or zero-day attacks [3].

[‡] *ORCID-ID:* `0009-0005-5221-1517`

[‡] *E-mail:* **yagneshnaidu1234@gmail.com**

Deep-learning approaches such as CNN, GRU, and LSTM networks have been employed in this context. To improve detection accuracy, hybrid models like CNN-GRU, CNN-LSTM, or GRU-CNN have also been proposed. The challenge of accurately detecting malicious patterns hidden among benign traffic is highlighted, reinforcing the motivation for this research using advanced hybrid models in IoT intrusion detection. Additionally, this research contributes to developing and evaluating hybrid architectures (CNN-GRU, CNN-LSTM and GRU-CNN), assesses performance using a real-world dataset, and evaluates trade-offs between performance and computational cost.

2. Related Work

The introduction of ML and DL techniques has primarily dominated research on the IDS for IoT networks [4]. Traditional technology, such as signature-based and rule-based IDSs, carries a high computational cost that cannot quickly adapt to new threats[5]. Recent advances in deep learning have introduced Convolutional Neural Networks (CNNs) for IDS. We use a type of RNN called GRUs and LSTM networks to capture temporal dependencies, which are very good at learning sequential attack patterns[6]. Hybrid deep learning models combining CNNs and RNNs have been explored to enhance IDS performance. Nevertheless, deep-learning-models are still not comprehensively compared systematically. In this paper, we contribute to filling the gaps by extensively evaluating these models on real-world IoT datasets. Studies have shown that hybrid deep learning models, like CNN-LSTM-GRU, can more effectively pinpoint intricate attack patterns such as Distributed Denial-of-Service (DDoS) [7]. CNN extracts spatial features, while LSTM and GRU capture short-term and long-term dependencies. [5]found enhanced accuracy in identifying network anomalies using CNN-GRU-based IDS. BiLSTM-based models balance computational efficiency and detection performance in resource-constrained IoT contexts. These models were validated in CICIDS-2017 and UNSW-NB15 [8] [9]. Researchers propose a GRU-LSTM fusion model to increase IoT security using GRU's short-term dependencies and LSTM's long-term pattern learning. Federated-Learning (FL)[10] is gaining traction as a privacy-preserving approach for IDS, enhancing scalability in large-scale IoT environments. CNN-GRU-based IDS models have been evaluated in fog computing environments, improving the detection performance of Mirai and Gafgyt bots and considering threat dynamics and changing behavioral patterns.

Figure 1 compares benign and malicious patterns in IoT traffic attack types. Unlike existing approaches, this research compares hybrid CNN-LSTM models to improve IDS mission critical solutions for IoT networks.

3. Methodology

3.1 *Dataset Acquisition and Preparation*

This study assessed the suitability of deep learning frameworks for anomaly detection in IoT networks, focusing on hybrid models that combine spatial and temporal capabilities for good performance. The dataset was generated in order to support the intrusion detection research in real-world IoT networks. It contains both normal and malicious traffic like Mirai and Gafgyt botnets [11]. The models were developed and trained

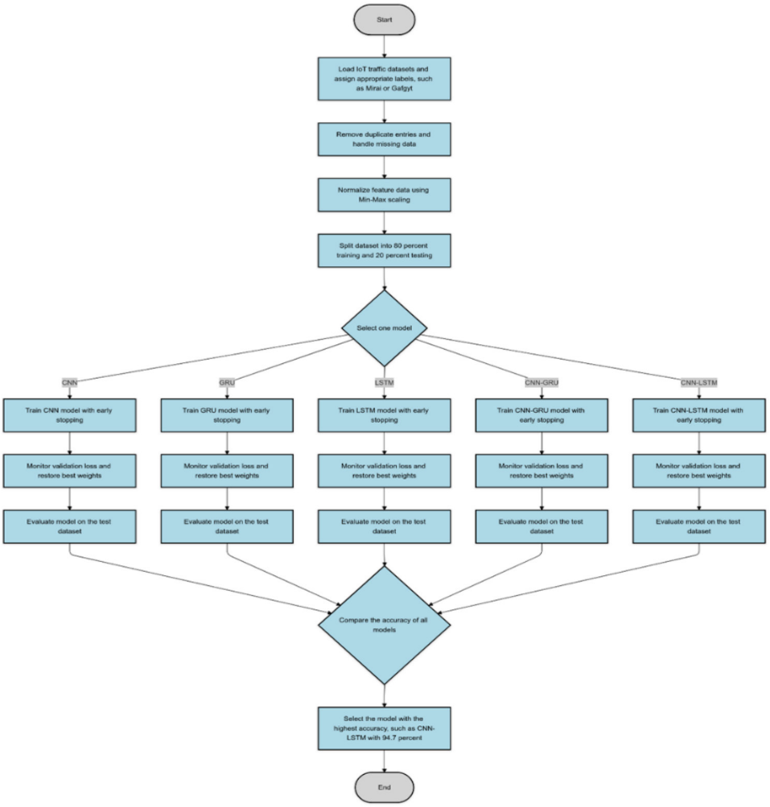

Start
Load IoT traffic datasets and assign appropriate labels, such as Mirai or Gafgyt
Remove duplicate entries and handle missing data
Normalize feature data using Min-Max scaling
Split dataset into 80 percent training and 20 percent testing
Select one model
CNN
GRU
LSTM
CNN-GRU
CNN-LSTM
Train CNN model with early stopping
Train GRU model with early stopping
Train LSTM model with early stopping
Train CNN-GRU model with early stopping
Train CNN-LSTM model with early stopping
Monitor validation loss and restore best weights
Monitor validation loss and restore best weights
Monitor validation loss and restore best weights
Monitor validation loss and restore best weights
Monitor validation loss and restore best weights
Evaluate model on the test dataset
Evaluate model on the test dataset
Evaluate model on the test dataset
Evaluate model on the test dataset
Evaluate model on the test dataset
Compare the accuracy of all models
Select the model with the highest accuracy, such as CNN-LSTM with 94.7 percent
End

Figure 1

Description of evaluated Models architectures.

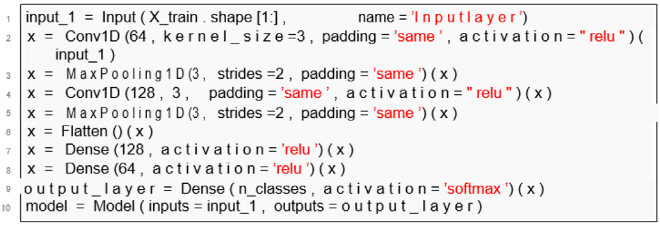
using TensorFlow, a popular deep-learning framework based on Python, with 70% data splitting for training, 15% validation, and 15% testing for generalizability. Additionally, it uses the Adam optimizer for training and employs a categorical cross-entropy loss function to handle multi-class classification. Furthermore, we managed to reduce overfitting through the use of batch normalization and dropout.

3.2 *Description of proposed Models*

Figure 1 outlines the operational procedures for the proposed hybrid deep learning models for IoT traffic classification. The process begins with importing and annotating datasets, preparing them by removing duplicates, and handling null entries. We clean the data, feature scale it using Min-Max Normalization, and then split our dataset into 80% for training and 20% for testing. Then, one of the five models, CNN, GRU, LSTM, or CNN-GRU, is selected, and CNN_LSTM Binary Cross entropy is used for training. The selected model is trained using an early stopping criterion to prevent overfitting. The model's accuracy is assessed across all five architectures to identify the optimal performing model.

3.3 *Composition of Evaluated Models and Implementation Strategies*

The study developed five deep learning models (CNN, GRU, LSTM, CNN-GRU, and CNN-LSTM) for IoT intrusion detection in network traffic. Key processes included data normalization using MinMaxScaler to scale feature values between 0 and 1, and the dataset was subdivided into training and testing while maintaining class label distribution. The 1D CNN model utilized a learning rate of 0.0005 with the Adam-optimizer and categorical cross-entropy as the loss function. The CNN-LSTM model achieved the highest classification accuracy of 94.7%. Early termination avoided overfitting by monitoring validation loss after five epochs. Listings 1 to 6 provide detailed model implementations.



```
input_1 = Input(X_train.shape[1:],          name='Inputlayer')
x = Conv1D(64, kernel_size=3, padding='same', activation="relu")(
    input_1)
x = MaxPooling1D(3, strides=2, padding='same')(x)
x = Conv1D(128, 3,  padding='same', activation="relu")(x)
x = MaxPooling1D(3, strides=2, padding='same')(x)
x = Flatten()(x)
x = Dense(128, activation='relu')(x)
x = Dense(64, activation='relu')(x)
output_layer = Dense(n_classes, activation='softmax')(x)
model = Model(inputs=input_1, outputs=output_layer)
```

Listing 1

CNN Architecture

```
model.add(GRU(128, return_sequences=True, input_shape=(X_train.
    shape[1], 1)))
model.add(GRU(64))
```

Listing 2

GRU Architecture

```
model.add(LSTM(128, return_sequences=True, input_shape=(X_train.
    shape[1], 1)))
model.add(LSTM(64))
```

Listing 3

LSTM Architecture

```
x = Conv1D(64, kernel_size=3, padding='same', activation='relu')(
    input_1)
x = MaxPooling1D(3, strides=2, padding='same')(x)
x = GRU(128, return_sequences=True)(x)
x = GRU(64)(x)
```

Listing 4

CNN-GRU Architecture

```
x = Conv1D(64, kernel_size=3, padding='same', activation='relu')(
    input_1)
x = MaxPooling1D(3, strides=2, padding='same')(x)
x = LSTM(128, return_sequences=True)(x)
x = LSTM(64)(x)
```

Listing 5

CNN-LSTM Architecture

```
early_stopping = EarlyStopping(monitor='val_loss', patience=5,
    restore_best_weights=True)
history = model.fit(X_train, y_train, epochs=10, batch_size=512,
    validation_split=0.2, callbacks=[early_stopping])

```

Listing 6

Training and Evaluation

4. Results and Discussion

The paper carefully assessed how the new model performed using “evaluation metrics” containing: accuracy, precision, recall rates and F1-Score. It also looked at how well the loss function converged. The CNN model experienced a fast initial reduction in loss, but the speed of improvement then declined, suggesting it was now training well. The GRU model showed a steady loss reduction, stabilizing halfway through training, but converged more slowly than CNN, requiring more epochs. The LSTM networks demonstrated a steady decrease in loss, stabilizing after 30 epochs, but faced issues with overfitting due to large scale and limited data. A combined CNN-GRU network achieved smoother training and faster convergence. In contrast, the CNN-LSTM hybrid outperformed others with higher accuracy and lower loss over epochs, exhibiting the smallest training-validation loss gap. Figures 2 to 6 illustrate these results. Tables 1 to 4 compare deep learning models for IoT intrusion detection, including performance metrics like accuracy, F1 score, recall, precision, execution times, and references to other studies with comparative analysis.

Table 1

Results of performance evaluation for the proposed Deep Learning Models.

Model	Accuracy	Precision	Recall	F1-score
CNN	94.2%	93.8%	94.1%	94.0%
GRU	94.3%	94.0%	94.4%	94.2%
LSTM	94.5%	94.3%	94.6%	94.5%
CNN-GRU	94.5%	94.4%	94.5%	94.5%
CNN-LSTM	94.7%	94.6%	94.7%	94.6%

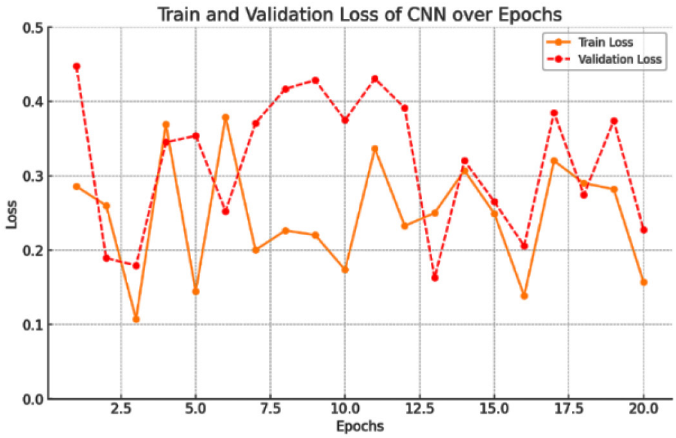


Figure 2

CNN Epoch Loss

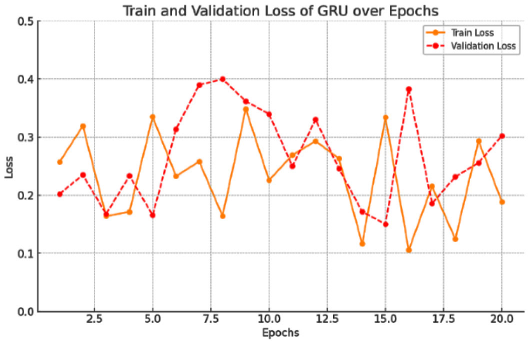


Figure 3

GRU Epoch Loss

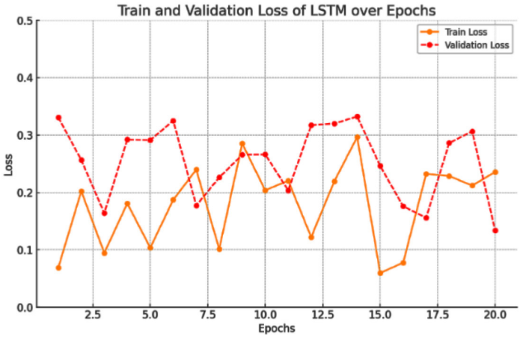


Figure 4

LSTM Epoch Loss

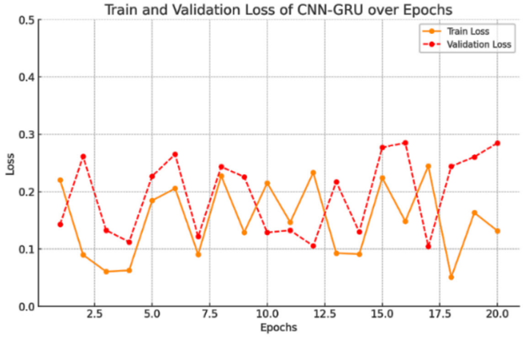


Figure 5

CNN-GRU Epoch Loss

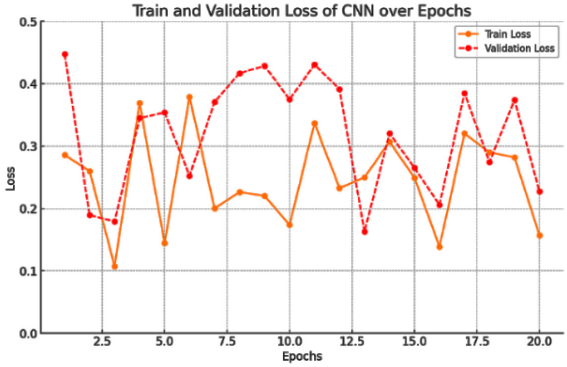


Figure 6

CNN-LSTM Epoch Loss

Table 2

Comparison of CNN and GRU Models considering our results with other studies.

Metric	CNN		GRU	
	Our	**Other**	**Our**	**Other**
Accuracy (%)	94.2	92.3	94.3	93.8
F1 Score	94.0	91.5	94.2	93.4
Recall	94.1	92.0	94.4	93.2
Precision	93.8	91.2	94.0	93.5
Dataset used	NB-IoT	CICIDS	NB-IoT	UNSW-NB15
Execution Time (seconds)	3.5	4.2	4.0	4.8
Paper/Journal		[5]		[12]

Table 3

Comparison of LSTM and CNN-GRU Models considering our results with other studies.

Metric	LSTM		CNN-GRU	
	Our	**Other**	**Our**	**Other**
Accuracy (%)	94.5	92.3	94.3	93.8
F1 Score	94.5	91.5	94.2	93.4
Recall	94.6	92.0	94.4	93.2

Contd...

Precision	94.3	91.2	94.0	93.5
Dataset used	NB-IoT	CICIDS	NB-IoT	UNSW-NB15
Execution Time (seconds)	4.2	5.0	4.8	5.3
Paper/Journal		[13]		[14]

Table 4

Comparing our combined CNN-LSTM model results with other studies.

Metric	CNN-LSTM	
	Our	**Other**
Accuracy (%)	94.7	94.2
F1 Score	94.6	94.0
Recall	94.7	94.1
Precision	94.6	94.0
Dataset used	NB-IoT	CICIDS
Execution Time (seconds)	5.1	5.6
Paper/Journal		[15]

5. Conclusion

This paper investigates DL systems architecture for IDS on IoT networks. The hybrid CNN-LSTM architecture, which combines convolutional feature extraction and sequence learning, has an accuracy of 94.7%. This architecture lowers false positives and increases detection rates. However, execution time, scalability, and resource limits impede real-world adoption. Future research should concentrate on optimization strategies, attention mechanisms, and federated learning to improve IDS efficiency and flexibility for strong cybersecurity in IoT networks [16].

References

[1] T. K. Mohammed, D. N. Vasundhara, S. H. Mehanoor, E. Sreedevi, P. R. Kumar, C. Manihass, and S. F. Baba, “A novel fusion approach for advancement in crime prediction and forecasting using hybridization of ARIMA and recurrent neural networks,” *Journal of Information*

Systems Engineering and Management, vol. 10, no. 38, pp. 404–420 (2025).

[2] B. Shilpa, P. R. Kumar, and R. K. Jha, "LoRa DL: A deep learning model for enhancing the data transmission over LoRa using autoencoder," *The Journal of Supercomputing,* vol. 79, no. 15, pp. 17079–17097 (2023).

[3] R. Q. Abdulkadhim, H. S. Abdullah, and M. J. Hadi, "Improving cryptocurrency price prediction through advanced LSTM-based deep learning techniques," *Journal of Statistics and Management Systems,* vol. 27, no. 8, pp. 1701–1712 (2024).

[4] V. Kantharaju, H. Suresh, M. N., S. Ansarullah, F. Amin, and A. Alabrah, "Machine learning based intrusion detection framework for detecting security attacks in internet of things," *Scientific Reports,* vol. 14 (2024).

[5] J.-M. Chen, "Multi-vendor and multi-buyer collaborative planning, forecasting and replenishment model," *Journal of Statistics and Management Systems,* vol. 28, no. 6, pp. 1023–1036 (2025).

[6] P. R. Kumar and B. Shilpa, "An IoT-based smart healthcare system with edge intelligence computing," in Reconnoitering the landscape of edge intelligence in healthcare, pp. 31–46, Apple Academic Press (2024).

[7] M. R. Z. E. Deen and G. M. Elmahdy, "Different types of odd harmonious labeling of super subdivision of various graphs," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2373–2407 (2024).

[8] B. Cao, C. Li, Y. Song, and X. Fan, "Network intrusion detection technology based on convolutional neural network and BiGRU," Computational Intelligence and Neuroscience (2022).

[9] R. Ranjan, D. Pandey, A. K. Rai, D. Gupta, P. Singh, P. R. Kumar, and S. N. Mohanty, "A manifold-level hybrid deep learning approach for sentiment classification using an autoregressive model," *Applied Sciences*, vol. 13, no. 5, pp. 3091 (2023).

[10] N. Thilakarathne, G. Muneeswari, P. V., F. Alassery, H. Hamam, R. Mahendran, et al., "Federated learning for privacy-preserved medical Internet of Things," *Intelligent Automation & Soft Computing*, vol. 33, pp. 157–172 (2022).

[11] B. Shilpa, P. R. Kumar, and R. K. Jha, "Spreading factor optimization for interference mitigation in dense indoor LoRa networks," in 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), pp. 1–5 (2023).

[12] G. Zhao, C. Ren, J. Wang, Y. Huang, and H. Chen, "IoT intrusion detection model based on gated recurrent unit and residual network," *Peer-to-Peer Networking and Applications,* vol. 16, pp. 1–13 (2023).

[13] I. Mani, Naveen, Anjana, and R. Bhardwaj, "Common fixed-point theorems satisfying rational contraction in partially ordered metric space," *Journal of Interdisciplinary Mathematics*, vol. 27, no. 8, pp. 1773–1779 (2024).

[14] Z. Al-Khuzaie, S. Albermany, and M. AbdlNibe, "Intrusion detection in the IoT-Fog adopting the GRU and CNN: A deep learning-based approach," pp. 379–389 (2023).

[15] P. R. Kumar and T. Ananthan, "Machine vision using LabVIEW for label inspection," *Journal of Innovation in Computer Science and Engineering,* vol. 9, no. 1, pp. 58–62 (2019).

[16] R. Q. Abdulkadhim, H. S. Abdullah, and M. J. Hadi, "Improving cryptocurrency price prediction through advanced LSTM-based deep learning techniques," *Journal of Statistics and Management Systems,* vol. 27, no. 8, pp. 1701–1712 (2024).

Received December, 2024