Cureus Journal of Computer Science

Open Access Original Article

Contextual Internet of Things Intrusion Detection: A Sliding Window Convolutional Neural Network–Gated Recurrent Unit Model Enhanced by Graph Neural Networks

Ramya Chinnasamy [1] , Malliga Subramanian [1] , Nandita Sengupta [2] , Ramkumar MP [3]

1. Computer Science and Engineering, Kongu Engineering College, Erode, IND 2. Information System, University College of Bahrain, Manama, BHR 3. Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, IND

Corresponding author: Ramya Chinnasamy, ramya.me@gmail.com

Received 04/29/2025
Review began 05/26/2025
Review ended 06/03/2025
Published 06/10/2025

DOI: https://doi.org/10.7759/s44389-025-06001-1

Abstract

The rapid expansion of Internet of Things (IoT) devices has introduced significant security challenges, particularly in detecting sophisticated cyber intrusions. This study proposes a novel hybrid deep learning framework combining convolutional neural networks, gated recurrent units, and graph neural networks to enhance intrusion detection capabilities in IoT environments. The model effectively captures spatial features, temporal dependencies, and inter-device relationships within network traffic data. Evaluated on the ToN-IoT dataset, the proposed system achieved a high classification accuracy of 98%, with an area under the curve and average precision score of 1.00, along with strong precision, recall, and F1-scores across both normal and attack classes. These results were obtained using an 80:20 train-test split, demonstrating the model's robustness and suitability for real-time deployment in intelligent and dynamic IoT-based intrusion detection systems.

Categories: Ensemble Learning, Network Security, IoT Security and Privacy
Keywords: intrusion detection systems(ids), internet of things(iot), cyber security, hybrid method, ton-iot dataset

Introduction

In recent years, the efficiency and automation of smart systems have been significantly enhanced due to the integration of Internet of Things (IoT) devices into modern infrastructure [1]. The smart systems include industrial control systems, intelligent transportation systems, and smart homes [2]. However, the unprecedented growth of IoT devices and networks makes the security a big gainsay, as discussed by Chinnasamy et al. [3]. These systems are vulnerable to a range of intrusions, from denial-of-service attacks and spoofing to more sophisticated multi-vector threats, as discussed by Tabassum et al. [4]. Traditional security solutions, including signature-based intrusion detection systems (IDSs), are often inadequate in detecting zero-day attacks and adapting to the evolving nature of cyber threats, as noted by Chinnasamy et al. [5]. Therefore, there is a growing need for intelligent, adaptive, and lightweight security mechanisms to protect these systems in real time, as highlighted by Qaddos et al. [6].

Zohourian et al. [7] discussed that deep learning-based IDSs have emerged as powerful tools for addressing these challenges. By leveraging their ability to learn complex and latent patterns within high-dimensional data, these models excel at identifying both known and previously unseen cyber threats [8]. Among the widely used architectures, gated recurrent units (GRUs), a variant of recurrent neural networks (RNNs), are particularly effective in capturing temporal dependencies within sequential data, such as network traffic [9]. Similarly, convolutional neural networks (CNNs), especially 1D-CNNs, are proficient at extracting local features from structured and time-series datasets [10]. A hybrid architecture combining GRUs and 1D-CNNs integrates the strengths of both, enabling robust temporal and spatial feature extraction [11]. However, these models often fail to capture inter-device relationships and contextual dependencies across IoT networks [12].

This study proposes an enhanced deep learning framework that integrates graph neural networks (GNNs) with a hybrid CNN-GRU model for intrusion detection in IoT networks. The framework addresses three core dimensions of IoT network security: temporal dynamics, spatial features, and inter-device relationships. Time-dependent features, such as device temperature and condition data, are pre-processed and segmented into time windows to form input sequences. GRU layers are employed to capture sequential correlations, while parallel CNN layers extract spatial features from the same inputs. In addition, GNN model captures both device-specific and network-structural dependencies, capturing the relational dynamics within the IoT ecosystem. This synergistic combination enhances the framework’s ability to identify complex attack patterns and understand contextual relationships between devices. The model is evaluated across various attack types, including reconnaissance, denial-of-service, injection, and spoofing attacks, showcasing its capability for fine-grained threat detection and improved intrusion

How to cite this article
Chinnasamy R, Subramanian M, Sengupta N, et al. (June 10, 2025) Contextual Internet of Things Intrusion Detection: A Sliding Window Convolutional Neural Network–Gated Recurrent Unit Model Enhanced by Graph Neural Networks. Cureus J Comput Sci 2 : es44389-025-06001-1. DOI https://doi.org/10.7759/s44389-025-06001-1

defence.

The major contributions of this research are as follows:

1. Introduction of a CNN-GRU-GNN Hybrid Framework: A novel deep learning architecture is proposed, integrating GRU and CNN layers with a GNN module. This combination captures temporal dependencies, spatial features, and inter-device relational dynamics, ensuring comprehensive IoT anomaly detection.

2. Relational Modeling Using GNNs: The GNN component introduces a new dimension to intrusion detection by explicitly learning the relationships and dependencies among IoT devices in the network.

3. Sliding-Window Methodology for Temporal Context: The study utilizes a sliding-window approach to segment time-series data, enabling the model to learn meaningful temporal patterns while preserving sequence continuity.

4. Standardized Preprocessing for Multi-Device Integration: Rigorous preprocessing techniques ensure consistency and uniformity across diverse IoT devices (e.g., smart refrigerators, GPS trackers, and thermostats), facilitating robust training and evaluation.

5. Comprehensive Performance Assessment: The framework is validated through an extensive suite of metrics, including confusion matrix, receiver operating characteristic (ROC) curves, and classification reports, demonstrating its effectiveness in detecting complex attack vectors.

Related works

Kilichev et al. [11] introduced an IDS for IoT-based electric vehicle charging stations, combining CNN, long short-term memory (LSTM), and GRU models to address complex cybersecurity challenges. The framework achieves outstanding accuracy, including 100% in binary classification and over 96% in multiclass scenarios. Alhayan et al. [13] introduced an Enhanced Anomaly Intrusion Detection using an Optimization Algorithm with Dimensionality Reduction and Hybrid Model technique, combining dimensionality reduction, machine learning, and deep learning models for anomaly-based intrusion detection in cybersecurity. Utilizing the CIC-IDS2017 dataset, this method achieved an impressive classification accuracy of 99.46%, surpassing existing approaches. Ishak et al. [14] presented a Cyberattack Defense Mechanism using Hybrid Transfer Learning with Snow Ablation Optimization Algorithm technique, leveraging hybrid transfer learning and optimization algorithms to enhance the cybersecurity of critical infrastructures. By combining CNN-bidirectional long short-term memory for classification and advanced optimization methods, it demonstrates superior performance through simulation validation on benchmark data. El-Shafeiy et al. [15] designed a deep complex gated recurrent network-based IoT network IDS, designed for IoT environments, that uses CNN for spatial feature extraction and complex gated recurrent networks for temporal feature analysis to enhance anomaly detection capabilities. Extensive evaluations on multiple datasets revealed its strong defense against cyberattacks, achieving an impressive detection accuracy of 99.2%. Lu et al. [16] proposed a novel IDS for communication-based train control systems, utilizing transfer learning with optimized 1D-CNN and LSTM to extract spatial and temporal features for detecting both known and zero-day attacks. It achieved high performance, with 99.32% accuracy for known attacks and 93.21% average F1-score for zero-day attack detection. Yin et al. [17] combined deep auto-encoder and capsule graph convolution with a sparrow search algorithm to enhance anomaly detection in 6G Internet of Everything by amplifying reconstruction error differences between normal and abnormal data. Experimental results validated its superior performance in distinguishing anomalies compared to other advanced methods. Nandanwar and Kartya [18] introduced AttackNet, an adaptive CNN-GRU deep learning model, for detecting and classifying botnet attacks in Industrial IoT (IIoT) systems with an accuracy of 99.75%, surpassing state-of-the-art techniques. It demonstrates superior performance on the N_BaIoT dataset, offering a robust solution to counter sophisticated cyber-attacks in IIoT environments.

Alrayes et al. [19] proposed a denoising autoencoder-based intrusion detection method for IoT systems, demonstrating exceptional accuracy and reliability in preventing unauthorized access. Evaluated using NSL-KDD and CICIDS 2017 datasets, the approach achieved outstanding performance metrics, enhancing cybersecurity measures across diverse IoT ecosystems. Karthikeyan et al. [20] presented a firefly algorithm with machine learning technique to significantly enhance intrusion detection accuracy in wireless sensor network aided by IoT systems, achieving a maximum accuracy of 99.34% using the NSL-KDD dataset. It highlighted the innovative integration of bio-inspired algorithms and machine learning as a robust security solution for safeguarding interconnected systems in critical sectors. Nanjappan et al. [21] introduced a DeepLG SecNet, an innovative approach combining LSTM, SecNet, and Crossover Chaos Game Optimization to enhance IoT security by detecting intrusions effectively. Validated on BoT-IoT and NSL-KDD datasets, it outperforms existing methods, showcasing superior accuracy, precision, recall, and F1-scores in safeguarding IoT ecosystems. Rahman et al. [22] explored the use of synthetic data generated through generative adversarial networks (GAN) to train machine learning models for Network NIDS, addressing issues like data imbalance and collection costs. The study demonstrates high performance

across datasets, achieving perfect scores of 100% on the BoT-IoT dataset and showcasing the potential of generative data in enhancing cybersecurity strategies. Wu et al. [23] developed an innovative squirrel search optimization-based Bengio Nesterov momentum convolutional neural network-based approach paired with HeInit-WGAN for intrusion detection in IoT networks, achieving good reliability and accuracy in mitigating security threats. With outstanding metrics like a precision of 0.96 and false positive rate of 0.02, it establishes a robust framework for safeguarding IoT environments against attacks. Table *1* presents a comparative summary of existing IDS approaches.

Author	Technique	Dataset	Accuracy (%)	Limitations Identified
Kilichev et al. [11]	CNN + LSTM + GRU	Custom (EVCS)	100 (binary), >96 (multiclass)	Lacks relational modeling; device-level contextual links missing
Alhayan et al. [13]	Hybrid DL + Feature Selection	CIC-IDS2017	99.46	Handles imbalance but overlooks inter-device relationships
Ishak et al. [14]	CNN-BiLSTM + SAOA	Benchmark datasets	Not reported	High complexity; no temporal sliding strategy used
El-Shafeiy et al. [15]	CNN + CGRN	Multiple IoT datasets	99.2	No GNN used; spatial-temporal relations only
Lu et al. [16]	Transfer Learning + 1D-CNN + LSTM	CBTC	99.32	Poor F1 for zero-day attacks (93.21)
Nandanwar et al. [18]	CNN-GRU (AttackNet)	N-BaIoT	99.75	Relational links and device context not modeled
Rahman et al. [22]	GAN-augmented ML	BoT-IoT	100	Focused on data synthesis; lacks real-time adaptability
Wu et al. [23]	HeInit-WGAN + CNN	IoT datasets	Precision: 96	High preprocessing overhead; no contextual awareness

TABLE 1: Comparative Summary of Existing IDS Approaches

IDS, Intrusion Detection System; CNN, Convolutional Neural Network; LSTM, Long Short-Term Memory; GRU, Gated Recurrent Unit; EVCS, Electric Vehicle Charging Stations; DL, Deep Learning; CIC-IDS2017, Canadian Institute for Cybersecurity Intrusion Detection System 2017 dataset; BiLSTM, Bidirectional Long Short-Term Memory; CBTC, Communications-Based Train Control; GAN, Generative Adversarial Network; ML, Machine Learning; HeInit, He Initialization; WGAN, Wasserstein Generative Adversarial Network; BoT-IoT, Botnet Internet of Things dataset; SAOA, Snow Ablation Optimization Algorithm; CGRN, Complex Gated Recurrent Network

Comparative discussion

Most existing IDS approaches utilize deep learning architectures such as CNNs, LSTMs, GRUs, or their hybrids to exploit spatial and temporal features within network traffic. However, a key limitation common to these methods is the lack of relational modeling - that is, they do not explicitly capture the contextual interdependencies between IoT devices, which are crucial in smart environments. Some techniques (e.g., Alhayan et al. [13], Rahman et al. [22]) tackle data imbalance and feature redundancy effectively but still fall short in modeling device-to-device interactions.

Additionally, while models like those of El-Shafeiy et al. [15] and Nandanwar et al. [18] achieve high accuracy, they operate primarily on independent samples, disregarding time-continuity and cross-device patterns. Others (e.g., Wu et al. [23]) incorporate synthetic data or advanced initializations, but do not scale well for real-time applications due to computational overhead.

Our proposed CNN-GRU-GNN hybrid framework addresses these gaps by:

• Incorporating GNNs to model device relationships, enabling contextual understanding.

• Applying a sliding window technique to preserve temporal continuity.

• Ensuring multi-device integration through standardized preprocessing, making the solution scalable and adaptable.

• Achieving an area under the receiver operating characteristic curve (AUC) and average precision (AP) of 1.00 and 98% overall accuracy, thus surpassing many prior works in both precision and recall.

In summary, there is a significant advancement in intrusion detection for IoT environments, utilizing techniques such as deep learning (e.g., CNN, LSTM, GRU), hybrid frameworks, optimization algorithms, and generative models to enhance detection accuracy and mitigate cyber threats. Despite these achievements, challenges persist in effectively capturing inter-device relationships, contextual dependencies, and ensuring scalability and real-time adaptability across diverse IoT ecosystems.

The proposed study addresses these gaps by integrating GNNs with a CNN-GRU hybrid framework to incorporate relational modeling of IoT devices, temporal dynamics, and spatial features. This approach ensures robust anomaly detection while overcoming limitations in existing methods, providing a comprehensive and adaptive security solution for IoT networks.

Materials And Methods

This section explicates the suggested method for building an effective IDS for IoT systems. It has four main areas: (i) dataset description, (ii) dataset preprocessing, (iii) model design, and (iv) performance evaluation, as shown in Figure *1*.

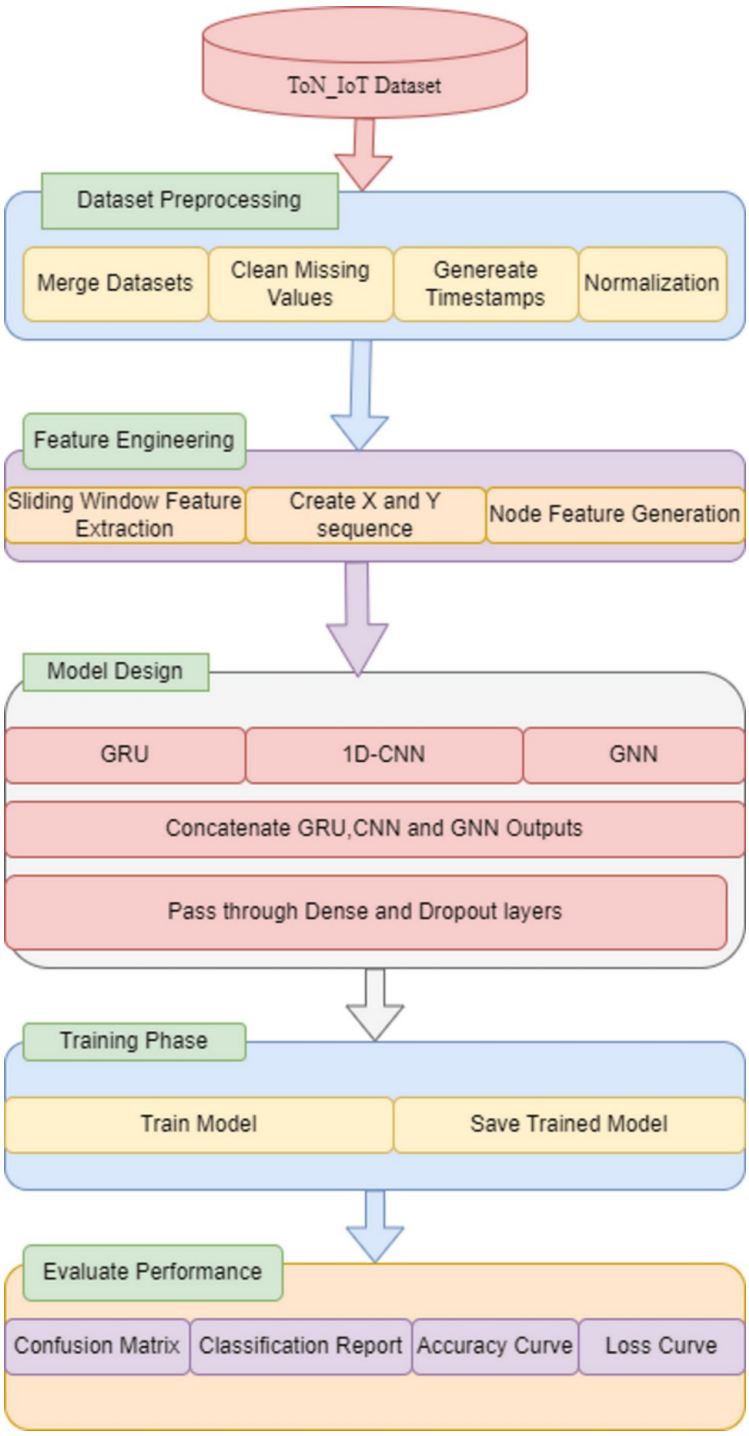

FIGURE 1: Proposed Method

GRU, Gated Recurrent Unit; CNN, Convolutional Neural Network; GNN, Graph Neural Network

Dataset description

The ToN-IoT dataset, developed by the Cyber Range Lab at UNSW Canberra, is a comprehensive benchmark for IoT security research, containing labeled data from multiple IoT devices, including smart fridges, thermostats, motion detectors, and weather sensors. This dataset captures real-world attack scenarios across various device types, making it suitable for developing and evaluating generalizable IDS models. Table *2* gives the details of the dataset, such as name of the dataset, features, various types of attacks along with their count and the total attacks. This dataset is available freely at https://research.unsw.edu.au/projects/toniot-datasets [24].

Name of the Dataset	Features Names	Attack Types	Count of Attack Types	Number of Instances
Train_Test_IoT_Fridge.csv	Date, time, fridge_temperature, temp_condition, label, type	{normal, ddos, backdoor, injection, password, ransomware, xss}	{15,000, 5,000, 5,000, 5,000, 5,000, 2,902, 2,042}	39,944
Train_Test_IoT_Garage_Door.csv	Date, time, door_state, sphone_signal, label, type	{normal, ddos, backdoor injection, password, ransomware, xss, scanning}	{15,000, 5,000, 5,000, 5,000, 5,000, 2,902, 1,156, 529}	39,587
Train_Test_IoT_GPS_Tracker.csv	Date, time, latitude, longitude, label, type	{normal, ddos, backdoor, injection, password, ransomware, xss, scanning}	{15,000, 5,000, 5,000, 5,000 5,000, 2,833, 577, 550}	38,960
Train_Test_IoT_Modbus.csv	Date, time, FC1_Read_Input_Register, FC2_Read_Discrete_Value, FC3_Read_Holding_Register, FC4_Read_Coil, label, type	{normal, injection, backdoor, password, xss, scanning}	{15,000, 5,000, 5,000, 5,000, 577, 529}	31,106
Train_Test_IoT_Motion_Light.csv	Date, time, motion_status, light_status, label, type	{normal ddos backdoor injection password ransomware scanning xss}	{15,000, 5,000, 5,000, 5,000, 2,264, 1,775, 449}	39,488
Train_Test_IoT_Thermostat.csv	Date, time, current_temperature, thermostat_status, label, type	{normal, injection, backdoor, password, ransomware, xss, scanning}	{15,000, 5,000, 5,000, 5,000, 2,264, 449, 61}	32,774
Train_Test_IoT_Weather.csv	Date, time, temperature, pressure, humidity, label, type	{normal, ddos, backdoor, injection, password, ransomware, xss, scanning}	{15,000, 5,000, 5,000, 5,000, 2,865, 866, 529}	39,260

TABLE 2: Dataset Description

Data preprocessing

The proposed framework processes telemetry and event logs from seven heterogeneous IoT devices: fridge, thermostat, GPS tracker, Modbus system, garage door, motion light, and weather sensor. Each device log undergoes the following standard preprocessing: (i) Time Unification: The date and time columns are stripped, concatenated, and converted into a single timestamp. (ii) Categorical features are converted into numeric values using label encoder. (iii) Temperature features from different devices are standardized into a unified feature named temperature. (iv) Missing or irrelevant features are filled with default values. (v) Data is normalized using min-max normalization.

Sliding window sequence generation

To capture temporal patterns, a fixed-length sliding window is applied across the unified dataset. Given a time-series of features $X_t\}_{t=1}^{N}$ and corresponding labels $y_{t}{}_{t=1}^{N}$, a window of size T produces sequence with Equation 1.

$$X_i = [x_i, x_{i+1}, x_{i+2}, \ldots, x_{i+T-1}] \in \mathbb{R}^{T\times d} \quad \text{and} \quad y_i = y_{i+T-1} \qquad (1)$$

where *d* is the feature dimension, *T* = 10, sliding window size, X_i is the input sequence, and y_i is the label of the timestamp.

The total number of sliding sample is given in Equation 2.

$$N_{\text{samples}} = N - T + 1 \qquad (2)$$

The sequences are then split into training and testing sets using an 80:20 stratified ratio.

1D CNN for spatial feature extraction

The CNN layer processes each time window to capture spatial features across time steps. Given an input sequence $S_i \in \mathbb{R}^{T\times d}$, the 1D convolution operation is defined with Equation 3.

$$h_j = \sigma\left(\sum_{k=0}^{K-1} w_k \cdot x_{j+k} + b\right), \quad j = 1, 2, 3, \ldots, T-K+1 \qquad (3)$$

where w_k is the kernel weight, *K* is the kernel size, *b* is the bias term, σ is the activation function, and h_j is the convolution at position *j*.

GRU for temporal sequence learning

The output of the CNN layer is fed into a GRU layer, which models the temporal dependencies in the sequence. Each GRU unit performs the following operations given in Equations 4-6 for input x_t at time *t*.

$$Z_t = \sigma\left(W_z x_t + U_z h_{t-1} + b_z\right) \qquad (4)$$

$$r_t = \sigma\left(W_r x_t + U_r h_{t-1} + b_r\right) \qquad (5)$$

$$\tilde{h}_t = \tanh\left(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h\right) \qquad (6)$$

where z_t and r_t are gates to control information flow, ▒ is the element-wise multiplication, h_t is the hidden state at time *t*, and *W*,*U* are weight matrices.

GNN for inter-device context modeling

To capture relationships between devices in the IoT network, a GNN layer is integrated. Each device is represented as a node in a graph G = (V,E), where V is the set of devices, and E is the set of communication or contextual edges. Each node $v_i \in V$ has a feature vector $h_i^{(0)}$ from CNN-GRU. The output of GNN uses the following Equation 7.

$$h_i^{(l+1)} = \sigma\left(\sum_{j\in N(i)} \frac{1}{C_{ij}} W^{(l)} h_j^{(l)}\right) \qquad (7)$$

where $h_i^{(l)}$ is the feature of node i at layer l, $N(i)$ is the neighborhood of node i, $W^{(l)}$ is the learnable weight matrix, C_{ij} is the normalization constant, and σ is the activation function.

Classification layer

The final representation from GNN is passed to a fully connected dense layer with softmax activation and is given by Equation 8.

$$\hat{y} = \sigma(WX + b) \qquad (8)$$

Loss function and optimization

The binary cross-entropy loss is calculated with Equation 9.

$$L_{\text{BCE}} = -\frac{1}{N}\sum_{i=1}^{n}\left[y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i)\right] \qquad (9)$$

where y_i denotes the true label, p_i the predicted probability, and *N* the total number of samples in a batch.

To optimize the model, the Adam optimizer is employed due to its adaptive learning rate and efficient convergence properties. A learning rate of 0.001 is used initially and reduced adaptively based on validation performance.

To prevent overfitting and ensure generalization, the following training strategies are applied:

Early Stopping: The training process is monitored using the validation loss. If the validation loss does not improve for 5 consecutive epochs, training is halted to avoid overfitting.

Dropout Layers: Dropout with a rate of 0.3 is applied after the CNN and GRU layers to reduce reliance on specific neurons and encourage more robust learning.

L2 Regularization: A small L2 penalty (\lambda = 1e^{-4}) is applied to the weights to discourage overly complex models.

Batch Normalization: This is applied after convolutional layers to stabilize learning and further reduce overfitting by normalizing the feature distribution across batches.

These techniques collectively contribute to the stability and generalization ability of the CNN-GRU-GNN hybrid framework, as evidenced by the close alignment between training and validation metrics shown in the results section.

Results

This section provides details about the results of the experiments conducted on the developed model and discusses the performance measures.

Accuracy

The accuracy curve for the proposed model is shown in Figure *2*, with validation accuracy over 97% within the first 10 epochs. The close alignment between training and validation accuracy throughout training indicates excellent generalization and minimal overfitting, a result of effectively modeling both temporal and spatial dependencies using GRU and CNN layers, respectively. The integration of GNN further strengthens contextual learning by capturing inter-device relationships, enabling the model to better differentiate between benign and malicious behavior. The model stabilizes after 10 epochs, maintaining consistent performance across subsequent iterations. These results demonstrate the model's robustness and adaptability in handling complex and dynamic IoT intrusion patterns.

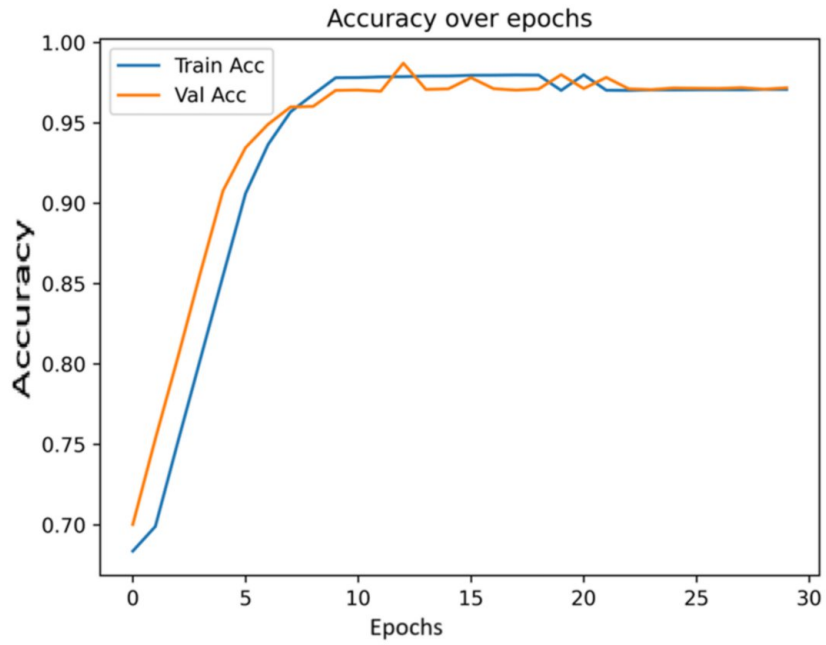

FIGURE 2: Accuracy Curve of the Proposed Model

Loss

The loss curve in Figure *3* illustrates a steady and rapid decrease in both training and validation losses during the initial epochs, reflecting efficient learning by the CNN-GRU-GNN hybrid model. By around epoch 10, both losses converge to values near zero, indicating that the model has effectively minimized prediction error. The small gap between training and validation losses demonstrates that the model generalizes well without significant overfitting. The occasional minor fluctuations in validation loss are

expected in complex models and do not impact overall stability. This consistently low loss across epochs confirms the model's robustness in accurately detecting intrusions in IoT environments.

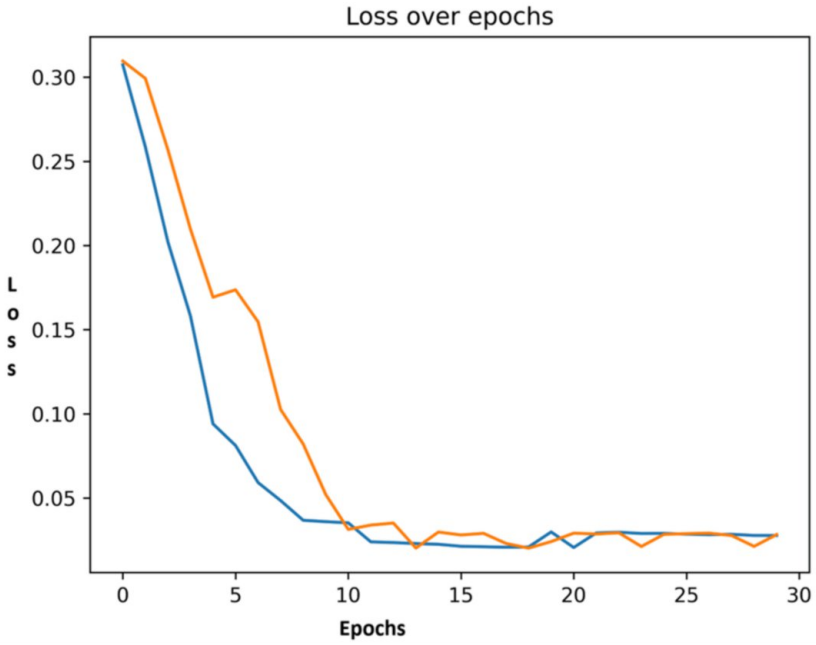

FIGURE 3: Loss Curve for the Proposed Model

Confusion matrix

The confusion matrix shown in Figure *4* highlights the strong classification capability of the proposed model, with 31,217 attack instances and 19,923 normal instances correctly classified. Only five attack samples were misclassified as normal, showing an exceptionally low false negative rate, which is critical in intrusion detection. However, 1,077 normal samples were incorrectly flagged as attacks, suggesting a slightly higher false positive rate, which may impact network performance due to unnecessary alerts. Despite this, the overall precision and recall are very high, indicating a well-balanced and reliable model. The results confirm that the hybrid CNN-GRU-GNN architecture effectively distinguishes between benign and malicious traffic in IoT environments.

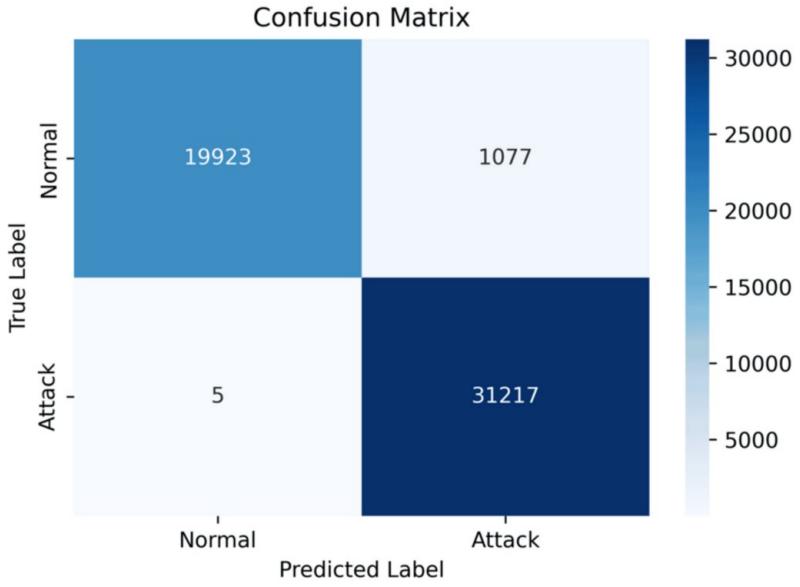

FIGURE 4: Binary Confusion Matrix of the Proposed Model

ROC curve

The ROC curve of the proposed CNN-GRU-GNN model shown in Figure *5* demonstrates an exceptional discriminative capability, with an AUC of 1.00, indicating perfect classification. This means the model achieves 100% true positive rate with 0% false positive rate at its optimal threshold, a highly desirable characteristic in IDS. The steep rise at the beginning of the curve and the flat top further reinforce the model's strong separation between attack and normal classes. This performance suggests no trade-off between sensitivity and specificity, highlighting the model's robustness and reliability. Such an outcome confirms the effectiveness of the integrated deep learning approach in learning complex attack patterns in binary classification tasks.

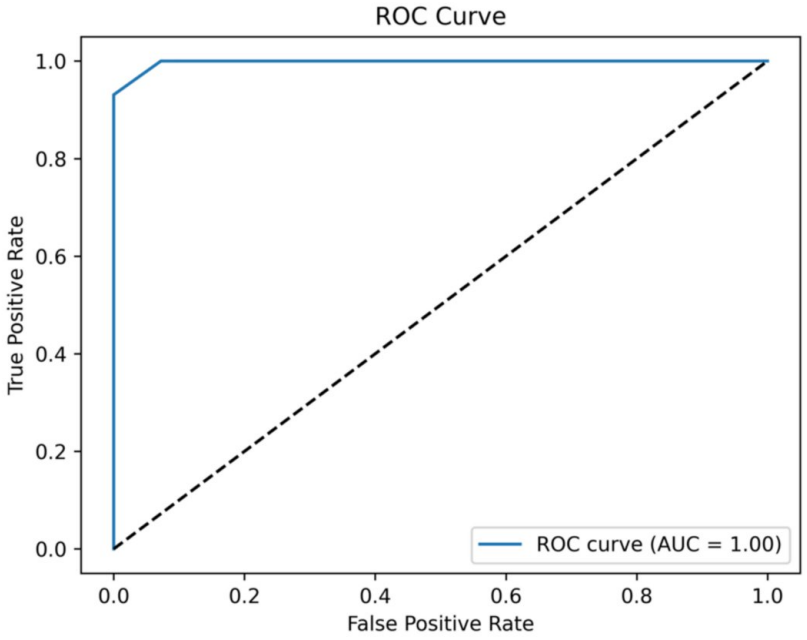

FIGURE 5: ROC Curve of the Proposed Model

AUC, Area Under the Curve; ROC, Receiver Operating Characteristic

Precision-recall curve

The precision-recall (PR) curve in Figure 6 highlights the near-perfect performance of the CNN-GRU-GNN model, with an AP of 1.00, indicating that the model successfully identifies nearly all actual attack instances with minimal false positives. The flat, high-precision region of the curve suggests that the classifier maintains excellent precision even at high recall levels, which is crucial in highly imbalanced datasets like intrusion detection. This robustness ensures that the model not only detects most attack attempts but does so without raising unnecessary alarms. High precision ensures reliability, while high recall ensures coverage.

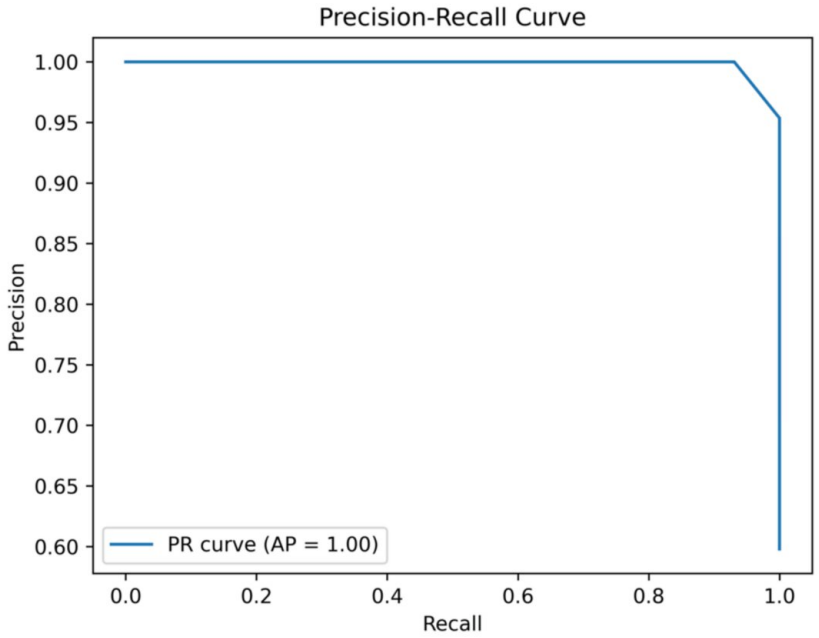

FIGURE 6: Precision-Recall Curve of the Proposed Model

AP, Average Precision; PR, Precision-Recall

Classification report

The proposed CNN-GRU-GNN hybrid model achieved outstanding performance on the ToN-IoT binary classification task, as shown in Table 3, with an overall accuracy of 98%. It demonstrated strong detection capability with a precision of 1.00 for Normal traffic and 0.97 for Attack traffic, while recall reached 1.00 and 0.95, respectively. The confusion matrix confirms the model's robustness, misclassifying only five attack samples out of 31,222 and 1,077 normal samples out of 21,000. Furthermore, the ROC and PR curves report AUC and AP values of 1.00, indicating excellent class separability and balance between precision and recall. These results highlight the model's effectiveness in detecting intrusions in the ToN-IoT environment.

	Precision	Recall	F1-score	Support
0	1.0000	0.95	0.97	21,000
1	0.97	1.0000	0.98	31,222
Accuracy			0.98	52,222
Macro avg	0.98	0.97	0.98	52,222
Weighted avg	0.98	0.98	0.98	52,222

TABLE 3: Classification Report of the Proposed Model

Discussion

This study presents a CNN-GRU-GNN hybrid deep learning model for binary intrusion detection on the ToN-IoT dataset. The model achieved an impressive overall accuracy of 98%, effectively distinguishing between normal and attack traffic. Despite the overall strong performance, the confusion matrix reveals that 1,077 normal instances were incorrectly flagged as attacks, indicating a false positive rate that may lead to unnecessary alerts in practical deployment. This misclassification could be attributed to several factors. First, feature overlap between benign and malicious behavior in certain IoT devices. Second, the class imbalance in the dataset, even after preprocessing, may have biased the model toward detecting attacks more aggressively. Third, contextual ambiguity in multi-device environments might lead to benign traffic being misinterpreted as coordinated malicious activity.

To mitigate this in real-world applications, several strategies are recommended:

• Threshold Tuning: Adjusting the decision threshold could help balance precision and recall for critical applications.

• Cost-Sensitive Learning: Incorporating misclassification costs can penalize false positives more heavily during training.

• Post-Detection Filtering: Introducing a secondary lightweight verification stage before raising alerts.

• Model Calibration: Using techniques like Platt scaling or isotonic regression can improve probability estimates and reduce overconfident misclassifications.

Precision and recall values were 1.00 and 0.95 for normal traffic, and 0.97 and 1.00 for attack traffic, respectively. The F1-scores of 0.97 (normal) and 0.98 (attack) further confirm the model's balanced performance. The ROC curve exhibits an AUC of 1.00, reflecting perfect discrimination capability between classes. Likewise, the PR curve achieved an AP score of 1.00, signifying minimal trade-off between precision and recall even with class imbalance. The model's ability to maintain high performance across multiple metrics proves its robustness and reliability. These results suggest the hybrid model effectively captures both spatial and temporal dependencies in network traffic. Ultimately, this architecture proves to be highly promising for real-world deployment in IoT and IoV IDSs.

Limitations and future work

While the proposed CNN-GRU-GNN framework demonstrated high performance on the ToN-IoT dataset, an important limitation is that only a single dataset was used for evaluation. Although ToN-IoT provides diverse IoT device logs and realistic attack scenarios, it does not capture the full spectrum of traffic characteristics, device heterogeneity, or emerging threats present in other public datasets (e.g., BoT-IoT, CIC-IDS2017) or real-world deployments. As a result, the generalizability of the model to unseen environments remains uncertain.

In future work, we plan to validate the model on multiple benchmark datasets with varying traffic profiles and attack types to assess cross-domain performance. Furthermore, real-world testing in edge or fog-based IoT environments will help identify practical deployment challenges, such as hardware constraints, noisy data, and live traffic dynamics. Incorporating transfer learning or domain adaptation techniques may also improve the model's adaptability across diverse contexts.

Conclusions

This study demonstrates the efficacy of a hybrid CNN-GRU-GNN architecture for intrusion detection using the ToN-IoT dataset. The proposed model achieved exceptional results, including 98% overall accuracy, near-perfect precision and recall, and an AUC and AP scores of 1.00. These outcomes highlight the model's robustness in identifying cyber threats with minimal false positives and false negatives. The architecture effectively learns spatial features using CNN, temporal patterns via GRU, and complex relational structures through GNN, making it suitable for dynamic IoT environments.

However, several practical deployment challenges must be addressed. First, the integration of GNNs, while powerful, introduces computational overhead and latency, which may hinder real-time detection in resource-constrained IoT devices. Second, scalability becomes a concern as the number of interconnected IoT nodes grows, potentially increasing the graph size and inference time. Third, deploying the model across heterogeneous IoT ecosystems with different data formats, communication protocols, and hardware capabilities presents integration complexity. Addressing these issues will require model optimization (e.g., pruning, quantization), edge-based deployment strategies, and modular interfacing to ensure seamless adoption within existing IoT infrastructures.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Ramya Chinnasamy, Malliga Subramanian, Nandita Sengupta, Ramkumar MP

Acquisition, analysis, or interpretation of data: Ramya Chinnasamy, Malliga Subramanian, Nandita Sengupta, Ramkumar MP

Drafting of the manuscript: Ramya Chinnasamy, Malliga Subramanian, Nandita Sengupta, Ramkumar MP

Critical review of the manuscript for important intellectual content: Ramya Chinnasamy, Malliga Subramanian, Nandita Sengupta, Ramkumar MP

Supervision: Malliga Subramanian, Nandita Sengupta

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Okey OD, Melgarejo DC, Saadi M, Rosa RL, Kleinschmidt JH, Rodríguez DZ: Transfer learning approach to IDS on cloud IoT devices using optimized CNN. IEEE Access. 2023, 11:1023-1038. 10.1109/ACCESS.2022.3233775
2. Hazman C, Guezzaz A, Benkirane S, Azrour M: Toward an intrusion detection model for IoT-based smart environments. Multimedia Tools and Applications. 2024, 83:62159-62180. 10.1007/s11042-023-16436-0
3. Chinnasamy R, Malliga S, Sengupta N: Deep learning-driven intrusion detection systems for smart cities-a systematic study. 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain. 2022, 79-84. 10.1049/icp.2023.0341
4. Tabassum A, Erbad A, Mohamed A, Guizani M: Privacy-preserving distributed IDS using incremental learning for IoT health systems. IEEE Access. 2021, 9:14271-14283. 10.1109/ACCESS.2021.3051530
5. Chinnasamy R, Subramanian M, Sengupta N: Designing of intrusion detection system using an ensemble of artificial neural network and honey badger optimization algorithm. 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD). 2023, 1-6. 10.1109/ITIKD56332.2023.10100161
6. Qaddos A, Yaseen MU, Al-Shamayleh AS, Imran M, Akhunzada A, Alharthi SZ: A novel intrusion detection framework for optimizing IoT security. Scientific Reports. 2024, 14:21789. 10.1038/s41598-024-72049-z
7. Zohourian A, Dadkhah S, Molyneaux H, Pinto Neto EC, Ghorbani AA: IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks. Computers & Security. 2024, 146:104034. 10.1016/j.cose.2024.104034
8. Chinnasamy R, Subramanian M, Sengupta N: Empowering intrusion detection systems: a synergistic hybrid approach with optimization and deep learning techniques for network security. The International Arab Journal of Information Technology. 2025, 22:60-76. 10.34028/iajit/22/1/6
9. Yue C, Wang L, Wang D, Duo R, Nie X: An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN. IEEE Access. 2021, 9:59527-59539. 10.1109/ACCESS.2021.3073413
10. Huang L, Li L, Wei X, Zhang D: Short-term prediction of wind power based on BiLSTM-CNN-WGAN-GP. Soft Computing. 2022, 26:10607-10621. 10.1007/s00500-021-06725-x
11. Kilichev D, Turimov D, Kim W: Next-generation intrusion detection for IoT EVCS: integrating CNN, LSTM, and GRU models. Mathematics. 2024, 12:571. 10.3390/math12040571
12. Riyaz B, Ganapathy S: A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft Computing. 2020, 24:17265-17278. 10.1007/s00500-020-05017-0
13. Alhayan F, Alshuhail A, Ismail AOA, et al.: Enhanced anomaly network intrusion detection using an improved snow ablation optimizer with dimensionality reduction and hybrid deep learning model. Scientific Reports. 2025, 15:13270. 10.1038/s41598-025-97398-1
14. Ishak MK: Mathematical modeling of cyberattack defense mechanism using hybrid transfer learning with snow ablation optimization algorithm in critical infrastructures. IEEE Access. 2025, 13:13329-13340. 10.1109/ACCESS.2025.3530931
15. El-Shafeiy E, Elsayed WM, Elwahsh H, Alsabaan M, Ibrahem MI, Elhady GF: Deep complex gated recurrent networks-based IoT network intrusion detection systems. Sensors. 2024, 24:5933. 10.3390/s24185933
16. Lu H, Zhao Y, Song Y, Yang Y, He G, Yu H, Ren Y: A transfer learning-based intrusion detection system for zero-day attack in communication-based train control system. Cluster Computing. 2024, 27:8477-8492. 10.1007/s10586-024-04376-9

17. Yin S, Li H, Laghari AA, Gadekallu TR, Sampedro GA, Almadhor A: An anomaly detection model based on deep auto-encoder and capsule graph convolution via sparrow search algorithm in 6G Internet of Everything. IEEE Internet of Things Journal. 2024, 11:29402-29411. 10.1109/JIOT.2024.3353337
18. Nandanwar H, Katarya R: Deep learning enabled intrusion detection system for Industrial IOT environment. Expert Systems with Applications. 2024, 249:123808. 10.1016/j.eswa.2024.123808
19. Alrayes FS, Zakariah M, Amin SU, Khan ZI, Helal M: Intrusion detection in IoT systems using denoising autoencoder. IEEE Access. 2024, 12:122401-122425. 10.1109/ACCESS.2024.3451726
20. Karthikeyan M, Manimegalai D, RajaGopal K: Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. Scientific Reports. 2024, 14:231. 10.1038/s41598-023-50554-x
21. Nanjappan M, Pradeep K, Natesan G, Samydurai A, Premalatha G: DeepLG SecNet: utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments. Cluster Computing. 2024, 27:5459-5471. 10.1007/s10586-023-04223-3
22. Rahman S, Pal S, Mittal S, Chawla T, Karmakar C: SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. Internet of Things. 2024, 26:101212. 10.1016/j.iot.2024.101212
23. Wu J, Haider SA, Yu H, Irshad M, Soni M, Bhadla MK, Zikria YB: An intelligent IoT intrusion detection system using HeInit-WGAN and SSO-BNMCNN based multivariate feature analysis. Engineering Applications of Artificial Intelligence. 2024, 127:107132. 10.1016/j.engappai.2023.107132
24. Moustafa N: A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society. 2021, 72:102994. 10.1016/j.scs.2021.102994