Journal of Information Systems and Telecommunication
Vol.13, No.2, April-June 2025, 130-138
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

# Designing a Hybrid Algorithm that Combines Deep Learning and PSO for Proactive Detection of Attacks in IoT Networks

Zahra Bakhshali [1], Alireza Pourebrahimi [2*], Ahmad Ebrahimi [3], Nazanin Pilevari [4]

[1].Department of Information Technology Management, SRC, Islamic Azad University, Tehran, Iran
[2].Department of Industrial Management, Karaj Branch, Islamic Azad University, Alborz, Iran
[3].Department of Industrial and Technology Management, SRC, Islamic Azad University, Tehran, Iran
[4].Department of Industrial Management, West Tehran Branch, Islamic Azad University, Tehran, Iran

Received: 02 Nov 2024 /Revised: 03 Apr 2025/ Accepted: 04 May 2025

**Abstract**

As a result, with the establishment of Internet of Things (IoT) at a booming pace, the demand for effective, green security systems to detect cyber-attacks is escalating. Despite thorough investigation in this domain, the heterogeneous nature and multifaceted characteristic of IoT data make successful attack detection a challenging task. This paper introduces a new method for enhancing IoT attack detection through a hybrid deep learning model (CNN-GRU-LSTM) integrated with Particle Swarm Optimization (PSO) for hyperparameter optimization. This methodology consists of different steps, starting with a CSV (Comma Separated Values) file to use it as the dataset, performing different data science operations like feature selection, calculating weights to balance the class for learning the model, etc. A hybrid CNN-GRU-LSTM model is subsequently established and trained with the integration of the merit of each algorithm: CNN for spatial feature abstraction, GRU for effectiveness in managing the sequential information, and LSTM for discovering the long-range dependencies. The hyperparameters of the PSO algorithm are optimized to find the best combination of features/parameters to improve detection performance and efficiency. The results show remarkable accuracy and efficiency improvements over traditional methods. H. PSO for Optimizing Hybrid Deep Learning Architecture The gainful approach to building deep neural networks for IoT frameworks is through PSO based improvements. The results help to advance a realm of research work in IoT security and lay a grouped foundation for further work in optimizing attack detection models with different machine learning algorithms and optimization approaches.

**Keywords:** Deep Learning Algorithms; Internet of Things; IoT Attacks; PSO Algorithm.

## 1- Introduction

The rapid development within the field of the Internet of Things (IoT) has impacted diverse industries, fostering clever automation and seamless connectivity. However, these technological trends have also posted tremendous demanding situations, in particular in protection. The protection of IoT networks is essential for protective sensitive data and preserving the integrity of related devices [1].

This takes a look at ambitions to enhance protection mechanisms in IoT networks with the aid of developing superior strategies for attack detection. Given the substantial increase inside the quantity of IoT gadgets and their applications, the importance of locating robust and green safety solutions has grown. IoT devices regularly face computational resource constraints, which reduce the effectiveness of traditional protection answers. These limitations necessitate using modern tactics which are each green and powerful.

Significant advancements were made in IoT protection. The use of deep studying algorithms, in particular combinations like CNN-GRU-LSTM, has proven excessive capability in identifying complicated styles and anomalies in big datasets [2]. Despite these advancements, considerable gaps remain in contemporary studies, specifically in addressing the problem of records imbalance. This has a look at seeks a hybrid technique that leverages the strengths of various deep getting to know fashions to better capture complex IoT visitors' patterns. Additionally, characteristic choice optimization the usage of the Particle Swarm Optimization (PSO) set of rules is employed, which will help enhance the accuracy and performance of the model in detecting assaults inside imbalanced records.

✉ **Alireza Pourebrahimi**
poorebrahimi@gmail.com

The number one goal of this research is to recommend a novel hybrid version for detecting assaults in Internet of Things (IoT) networks. This hybrid version, which integrates deep gaining knowledge of architectures consisting of CNN, GRU, and LSTM, is designed to enhance accuracy and performance in attack detection. Additionally, the Particle Swarm Optimization (PSO) set of rules is utilized for function choice optimization, helping in the effective management of problems springing up from statistics imbalance. The studies additionally compare the proposed version with present techniques like RNN, LSTM-RNN, GRU, and GRU-CNN to demonstrate the innovation and efficacy of the proposed version.

**Research Contributions**

This observe gives numerous tremendous contributions to the field of assault detection in IoT networks:

- Modeling Innovation: The advent of a hybrid version primarily based on CNN, GRU, and LSTM, which significantly improves the potential to locate complicated patterns and anomalies in IoT visitors.
- Hyperparameter Optimization: The use of PSO for feature selection optimization, which no longer best will increase detection accuracy however also reduces the computational complexity of the version. This technique is especially effective in addressing facts imbalance, enhancing the model's efficiency in detecting rare but crucial assaults.
- Empirical Evaluation: A comprehensive assessment of the proposed model with current methods, providing empirical evidence of the proposed model's superiority and excessive efficiency, laying the foundation for the development of greater advanced protection systems within the IoT domain.

**Organization of the Paper**

- Section 2: Review of previous works in attack detection of IoT networks and deep learning techniques;
- Section 3: Proposed hybrid model is explained in detail with an elaboration of the process of feature optimization using PSO;
- Section 4: The Used datasets and preprocessing methods are explained;
- Section 5: Results of experiments with an illustration of the performance of the proposed model compared to existing methods.
- Section 6: Discussion and conclusion: This includes recommendations for possible future research.

## 2- Related Work

The current section is focused on research into IoT network attack detection, especially that related to deep learning algorithms applied within this domain. Original advanced approaches in machine learning and artificial intelligence aimed at raising the accuracy and efficiency of anomaly and cyber-attack detection in IoT environments are introduced and reviewed herein. The paper reviews recent research in comparison with older methods for these technologies that have impacts on increasing the detection power and reducing error rates in IoT networks.

In [3] reviews and compares some deep learning methods in intrusion detection in IoT devices. In this paper, different deep learning models were experimented with: Convolutional Neural Networks, Long Short-Term Memory networks, and Gated Recurrent Units. The results empirically show that these methods can be efficiently applied for attack detection in IoT environments. One of the main contributions of this research will be to introduce a proposed model for intrusion detection that will show high accuracy compared with the existing methods. In the methodology of this research, the implementation and evaluation of these models will be done using standard datasets for intrusion detection. It also discusses the limitations like extensive training data and a long training time for the models. It finally concludes that the deep learning models have some promise in improving attack detection, shows suggestions for future studies for classifying other variables, and improves the performance of the models.

In [4] deals with the investigation of a new model to detect attacks in the IoT environment. It applies deep learning techniques by proposing the combining scheme of optimization algorithms with Recurrent Convolutional Neural Networks to improve accuracy in detection. This paper offers two main contributions: the development of the RKCNN-MMBO model that showed a very high accuracy rate in attack detection. The limitations of the research are the large volume of data needed for the purpose of accurate model training and its high computational complexity. It highly emphasizes the efficiency of the RKCNN-MMBO model in improving the attack detection capability in IoT, accompanied by some suggestion for future work.

The article "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System" [5] investigates and develops an intrusion detection system using a hybrid deep learning model consisting of Convolutional Neural Networks and Recurrent Neural Networks. The paper presents a proposed intrusion detection system that can predict and classify cyber-attacks Bloomfield and Nelson, the major contribution of this paper is the proposal of the HCRNNIDS model; it has an accuracy rate in attack detection as high as 97.75% with ten-fold cross-validation. The methodology used is based on the combination of convolutional neural network methods for the extraction of local features and recurrent neural network methods for the capture of temporal features in order to improve IDSs. The paper also discusses the limitations related to the extensive training data needed and the computational complexity in the accurate training of the model. The conclusion comments on the fact that the

proposed HCRNNIDS model outperforms existing methods and can be taken as a new way of attack prediction in computer networks.

In [6] investigates the use of a BRNN for intrusion detection in IoT devices. In this paper, the considerable contributions made were related to the design of a BRNN model processing information from both temporal directions simultaneously: past and future, improving attack detection accuracy drastically. The methodology of the research also includes techniques for feature selection and parameter optimization using the Random Forest algorithm to increase model accuracy. Some limitations include that large datasets are needed for the proper training of the models, and in itself, BRNN has high computational complexity. The main contribution and conclusion are that the BRNN model outperforms conventional RNN and GRNN models and can be an effective security solution in IoT environments.

In [7] proposes an intelligent intrusion detection framework with deep learning algorithms for IoT networks. In the hybrid model, this paper uses RNN-GRU and can detect attacks on three layers: physical, network, and application. The steps performed in the research methodology include data preprocessing through cleaning, feature encoding, filtering, combining, and normalization. The self-imposed limitations in the study include that accurate training requires large datasets and high computational complexity. Considering such advantages, this method has to turn out much better than existing models.

The authors in [8] conducted research on using machine learning and deep learning to solve security problems in the internet of things (IoT) system. The research does the filtering of IoT threat video with the help of attack models for the initial attacks detection, to extract network traffic data for training the feature as well as for the database driven features for the detection of attacks. The accuracy is better, computational time is low with higher recall and G-mean. The paper also described category of algorithms including classification of CNNs and comparison between the accuracy and time run between them. It outlines the privacy and security in the IoT system and how ML and DL algorithm can guarantee those security and privacy.

In [9], a deep learning based GRU-RNN is developed for intrusion detection in SDN environment. Only 6 raw features from the NSL-KDD dataset is used to achieve accuracy of 89%. Experimental results confirm that the proposed approach does not impact network performance and therefore makes it a practical option for intrusion detection in SDN environments. The proposed GRU-RNN demonstrates that intrusion detection in SDN environments generated from the NSL-KDD dataset has an accuracy of 89%, which is better than other algorithms VanilaRNN, SVM and DNN in terms of Precision (P), Recall (R), F-measure (F) and Accuracy (AC). The suggested GRU-RNN reported a detections of 89% and 90% are raw footprints benign and anomalies, 0-day attacks exceed accuracy, Certainly, the GRU-RNNs method has directed better TPR and low FPR when compared with other algorithms, it also proved to have lesser false positive rate which is very congeal to a IDS. The proposed GRU-RNN model achieves an AC of anomaly detection of 89%, which is an enhancement over algorithms such as SVM, DNN, and NB Tree.

Table 1: Focus area, methodology, dataset, and major findings for the surveyed articles.

Table 1: Review of Articles

| Title of the Paper | Key Findings | Dataset Used | Main Method | Focus Area |
|---|---|---|---|---|
| Intrusion Detection in IoT Using Deep Learning [3] | Deep learning models like CNN, GRU, and LSTM have shown high accuracy in detecting attacks. | N-BaIoT | CNN, GRU, LSTM | Attack detection in IoT |
| Intrusion Detection Model for IoT Using Recurrent Kernel Convolutional Neural Network [4] | The RKCNN-MMBO model has demonstrated very high accuracy in attack detection. | CICIDS-2017 | RKCNN-MMBO | Cyber-attack detection |
| HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System [5] | Results indicate the superiority of the HCRNNIDS model with high accuracy in attack detection. | CSE-CIC-DS2018 | CNN, RNN | Attack detection in IoT |
| Bi-directional Recurrent Neural Network for Intrusion Detection System (IDS) in the Internet of Things[6] | Using BRNN has significantly improved attack detection accuracy. | UNB ISCX 2012 | BRNN | Attack detection in IoT |
| A Hybrid Deep Learning-Based Intrusion Detection System for IoT Networks [7] | The hybrid RNN-GRU model performs with high accuracy (up to 85%) in detecting attacks and outperforms other IDS models. | ToN-IoT | RNN-GRU | Attack detection in three-layer IoT architecture |
| Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems[8] | High accuracy, low false alarm rate, effective distinction between traffic types | NSL-KDD | LSTM-RNN algorithm | Identification system using LSTM-RNN |
| Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks [9] | High accuracy, low false alarm rate, effective distinction between traffic types | NSL-KDD | LSTM-RNN architecture | Identification system using LSTM-RNN |

## 3- Background and Explanation

Cybersecurity within the Internet of Things grew and is still growing to become the most critical issue in the domain of Information Technology, as the number and diversity of devices connected with the advent of their various wide-range applications grow drastically. In general, IoT allows devices and systems to communicate with each other and share data over the internet [10]. While stimulating a wide array of processes, it also opens up new security threats that need special attention. Notably, detection and countering cyber-attacks are some of the challenges that naturally come along with these kinds of networks and have turned into an obstacle [11].

The researchers have been working substantially in the security of the IoT devices for the past years. Since the concept concerned researchers, ways to protect those devices from attacks have been found. The first efforts that were put in were initially traditional security methods, like firewalls, Intrusion Detection Systems, among others. All these methods proved insufficient due to the enormous volume and complexity of data involved. Due to advancement in technologies and innovations in machine learning and deep learning algorithms, more advanced approaches for attack detection have been developed that can analyze and process large volumes of data more accurately.

Deep learning algorithms have evolved to become an industry standard in the process of intrusion detection in any IoT network today [12]. Challenges like class imbalance and the requirement for exact feature optimization, however, still exist to a great extent. In this paper, these have been addressed through the use of PSO.

Particle Swarm Optimization algorithm is a population-based optimization method, inspired by the collective behavior of birds and fish [13]. It considers a swarm of particles moving through the search space to search for the optimal solution. Each particle thus updates the position based on its experience and experience of other particles, which converges finally to get the best solution [١٤]. In this work, PSO is applied for selecting key features from IoT data in order to enhance the accuracy and efficiency of deep learning models.

Below is the pseudocode and flowchart of the particle swarm optimization algorithm.

| Pseudocode for Particle Swarm Optimization (PSO) |
|---|
| 1. Initialize parameters:<br>- Define the number of particles.<br>- Define inertia weight, cognitive constant, and social constant.<br>- Initialize the position of each particle randomly.<br>- Initialize the velocity of each particle randomly.<br>- Initialize the best known position (pBest) for each particle to its initial position.<br>- Initialize the global best position (gBest) to the best initial position among all particles.<br><br>2. Evaluate:<br>- Calculate the fitness value for each particle based on the objective function.<br>- If a particle's current position is better than its pBest, update pBest to the current position.<br>- If a particle's current position is better than the gBest, update gBest to the current position.<br><br>3. Update velocity and position:<br>- For each particle, update its velocity using the formula:<br>velocity = inertia * velocity + cognitive * random() * (pBest - position) + social * random() * (gBest - position)<br>- Update the position of each particle using the formula:<br>position = position + velocity<br><br>4. Check termination criteria:<br>- If the stopping criterion (e.g., maximum number of iterations or desired accuracy) is met, stop the algorithm.<br>- Otherwise, go back to step 2.<br><br>5. Output:<br>- The global best position (gBest) is the solution to the optimization problem. |

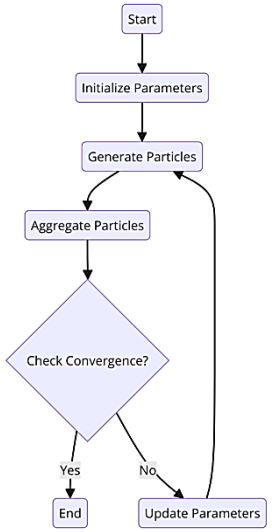


Fig. 1 Particle Aggregation Algorithm Flowchart [13]

## 4- Model and System Framework

The main aim of this paper is to enhance the capability of fast and accurate detection of attacks on IoT networks to prevent any system problem. In this regard, we consider the application of the following deep learning algorithms: Convolutional Neural Network, Gated Recurrent Unit, and Long Short-Term Memory. Besides, in the process of hyperparameter optimization, the work applies the algorithm of particle swarm optimization. The details of the

proposed approach are summarized below and further elaborated with the help of a pseudocode representation

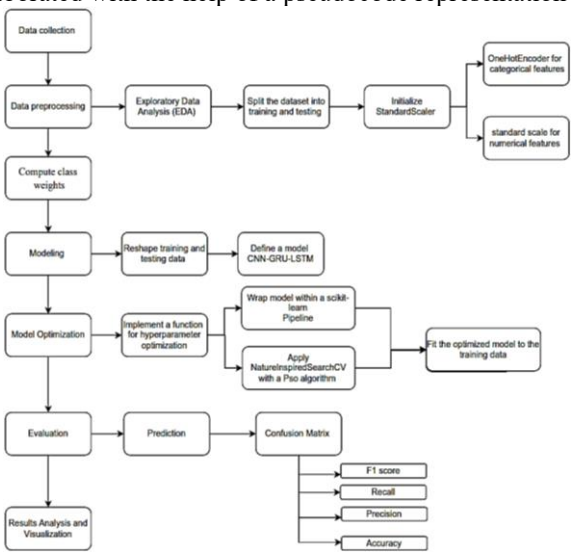


Fig. 1 Flowchart of the proposed method (researcher)

| Pseudo Code |
|---|
| 1. Data Collection<br>- Collect data from the source.<br>2. Data Preprocessing<br>- Perform Exploratory Data Analysis (EDA).<br>- Split the dataset into training and testing sets.<br>- Initialize StandardScaler for numerical features.<br>- Apply OneHotEncoder for categorical features.<br>3. Compute Class Weights<br>- Calculate class weights for handling class imbalance.<br>4. Modeling<br>- Reshape training and testing data as needed.<br>- Define the CNN-GRU-LSTM model architecture.<br>- Wrap the model within a scikit-learn Pipeline.<br>5. Model Optimization<br>- Implement a function for hyperparameter optimization.<br>- Apply NatureInspiredSearchCV with a Particle Swarm Optimization (PSO) algorithm.<br>- Fit the optimized model to the training data.<br>6. Evaluation<br>- Make predictions using the optimized model.<br>- Compute and display the Confusion Matrix.<br>7. Results Analysis and Visualization<br>- Calculate evaluation metrics: F1 score, Recall, Precision, and Accuracy.<br>- Visualize the results using appropriate plots. |

In this look at, we gift a complete gadget version and framework for developing and comparing a hybrid CNN-GRU-LSTM model aimed at improving intrusion detection skills in Internet of Things (IoT) networks. This technique leverages Convolutional Neural Networks (CNN), Gated Recurrent Units (GRU), and Long Short-Term Memory (LSTM) networks to address the complexity and evolving nature of safety threats in networked environments.

The initial segment of our methodology entails statistics series and preprocessing the use of the UNSW_NB15 dataset, a widespread dataset hired in network intrusion detection research. The records undergo preprocessing steps which include disposing of identifier columns and encoding the goal column the use of LabelEncoder to convert specific labels into numerical format appropriate for version processing. Missing values are handled to ensure that no facts gaps affect the schooling system. Additionally, numerical functions are normalized the usage of StandardScaler, and express functions are converted using OneHotEncoder to put together the records for powerful model input.

Exploratory Data Analysis (EDA) is conducted to study elegance distribution and pick out any imbalances that might bias the version's education and prediction accuracy. To mitigate the effect of class imbalance on model overall performance, elegance weights are calculated primarily based at the inverse frequency of class occurrences within the schooling statistics. This method guarantees a balanced education surroundings, allowing the version to analyze equitably across all class labels.

The model structure is designed to leverage the strengths of both convolutional and recurrent neural network technologies. The version starts off evolved with an preliminary convolutional layer that applies convolution operations to capture spatial hierarchies and functions from the input records, followed by using a max pooling layer that reduces records dimensionality, thereby decreasing model complexity without dropping vital facts. Subsequent layers consist of GRU and LSTM units, which excel at taking pictures temporal dependencies and long-time period relationships in the information, critical for detecting complex intrusion sports over the years. The community concludes with a Dense layer that transforms the processed features into the final output used for class.

We tune or optimize our model using a nature-inspired algorithm, particularly the Particle Swarm Optimization algorithm. This algorithm will help in hyperparameter tuning by guided search in the parameter space through the social behavior of a flock of birds for finding an optimum solution in a natural way. Hence, this step-in optimization is important to adapt the unique characteristics of the dataset, as the model would learn such characteristics and performances in this dataset, hence augmenting its accuracy and generalization capability.

Model performance assessment is performed in terms of several metrics, such as mean squared error, mean absolute error, R-squared values, and the correlation coefficient between the predicted and actual values. All these metrics give an in-depth understanding of predictive models in terms of their accuracy and efficiency. Evaluation confirms the model's ability to generalize to new, unseen data and also shows that it can be very useful in a real-world scenario

where one needs a reliable and robust intrusion detection system.

In this respect, the present study has developed a very potent framework of intrusion detection in Internet of Things networks by implementing newer concepts of machine learning and optimization algorithms. The combination of an integrated model of CNN, GRU, and LSTM further optimized with PSO makes the scheme very effective in managing major challenges in the respective field and opens further avenues for enhancing network security technologies. That is to say, the embedding of these two deep learning architectures could be a giant leap in the development of adaptable, efficient, and accurate security systems against a sequence of attacks within any setup of a complex network.

**Data Used for Simulations**

Through this research, UNSW-NB15 dataset. This data set of raw network packets was generated by the IXIA PerfectStorm device in UNSW Canberra Cyber Range Lab. This dataset was used to provide a complete set of new normal activities and synthetic attack behaviors. The features considered in this data are vast in number, including those directly extracted from network traffic, such as IP addresses, ports, protocols, temporal ones, and transferred volumetric data.

## 5- Findings and Results Analysis

In this paper, we designed and carried out a singular hybrid deep mastering algorithm for proactive assault detection in Internet of Things (IoT) networks. This hybrid set of rules makes use of CNN, GRU, and LSTM architectures and enhances its performance the use of Particle Swarm Optimization (PSO) for hyperparameter choice. To evaluate the efficiency of this hybrid model, we compared it with RNN, LSTM-RNN, GRU, and GRU-CNN algorithms. This assessment is primarily based on 4 number one evaluation metrics: accuracy, precision, bear in mind, and F1 score. These metrics enable us to evaluate the model's ability to accurately detect assaults in real-world environments with imbalanced records.

1. Accuracy:
- It is the metric that estimates how accurate is the algorithm in detecting attacks and non-attacks [15].

$$\text{Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}} \quad (1)$$

2. Precision:
- This metric measures the proficiency of the algorithm in raising an alarm when an attack has really taken place [16].

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (2)$$

3. Recall:
- This metric measures the set of rules's fulfillment in identifying real assaults as compared to the total real assaults [17].

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \quad (3)$$

4. F1 Score:
- This metric combines precision and recall to symbolize the balance between these two measures [17].

$$\text{F1 Score} = \frac{2\times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

In this phase, we gift the parameters and hyperparameters used to optimize the PSO set of rules. The intention of this optimization is to successfully track the parameters of the hybrid CNN-GRU-LSTM version to reap the highest accuracy in detecting attacks in IoT networks.

Table 2: Hyperparameters Used in the Model

| Functional Parameter | Values |
|---|---|
| Activation Function | RELU, SELU |
| Neurons per Layer | 75, 150 |
| Regularization | L1, L2 |
| Learning Rate | 0.001, 0.004 |

These are carefully chosen hyperparameters so that the model is estimated to be able to capture all complex patterns that might be intrinsic in IoT network traffic data. Moreover, we considered additional activation functions, regularization settings, number of neurons per layer, and learning rates for examining their role in the overall performance of the model and choosing the best one to provide the highest detection accuracy.

This paper shows that many critical hyper-parameters can be optimized for optimal performance of a Hybrid CNN-GRU-LSTM model designed for attack detection in IoT networks. These were opted such that the possibilities of overfitting reduce with optimum performance of the model.

Activation Function: We considered not unusual activation features, RELU and SELU, to be used in distinctive layers of the neural community. These capabilities were selected for their capability to help accelerate community convergence and reduce the vanishing gradient problem.

Regularizes: To cope with overfitting, two sorts of regularizes, L1 and L2, have been employed. These regularizes help the version by means of diminishing insignificant weights and preserving most effective meaningful functions.

Neurons in keeping with Layer: Based on trial and error, neuron counts have been decided on: 75 and 150. This configuration permits for modeling the complexities of IoT information by means of presenting sufficient flexibility to the community.

Learning Rate: Two mastering fees, zero.001 and 0.004, were used to alter the velocity of weight updates throughout the education process. Different learning charges permit us to find the right balance among gaining knowledge of velocity and version accuracy.

Below, Table 3 presents the parameters used by the PSO set of rules.

Table 3: PSO Algorithm Parameters

| Parameter | Description | Selected Values |
|---|---|---|
| w | Inertia coefficient controlling the influence of previous motion of particles | 0.7 |
| c1 | Personal coefficient that determines the attraction of particles to their best, previously found position. | 1.5 |
| c2 | Social coefficient relating particle attraction strength to the group's global best position | 1.5 |
| v_min | Minimum particle velocity, which constrains the possible movement of particles in the search space of a problem | -1 |
| v_max | The maximum velocity of particles, thus limiting the maximum perturbation of a particle within the search space. | 1 |

These parameters have been tuned in a way that balances the exploration and exploitation of the search space so that PSO algorithm would find the global optimal set of parameters for which the model would elude local minima and improve in convergence rate for proactive attack detection in IoT networks.

Results after running the PSO algorithm were the best values selected, stored, and used in training the final model. Parameters optimized by PSO are shown below.

Table 3: PSO algorithm parameters

| Parameter | Selected Value |
|---|---|
| Activation Function | RELU |
| Neurons per Layer | 150 |
| Regularization | L2 |
| Learning Rate | 0.001 |
| w (Inertia) | 0.7 |
| c1 (Personal Coeff.) | 1.5 |
| c2 (Social Coeff.) | 1.5 |
| v_min (Min Velocity) | -1 |
| v_max (Max Velocity) | 1 |

Table 4: Best Values Selected Using the PSO Algorithm

| | | | |
|---|---|---|---|
| L1 | Regularizes | RELU | Activation Function |
| 0.001 | Learning Rate | 150 | Neurons per Layer |

We now gift the results from the training and checking out levels of the model, illustrated via performance statistics. This information demonstrates how the hybrid CNN-GRU-LSTM model, utilizing superior optimization algorithms and deep learning, has completed excessive accuracy in detecting assaults in IoT networks. The outcomes from each the training and trying out facts are special within the desk below, highlighting the version's success in each phase.

Table 5: Model Performance Results on Training and Testing Data

| Metric | Training Data | Testing Data |
|---|---|---|
| Accuracy | 93.8% | 93.24% |
| Precision | 90.3% | 89.00% |
| Recall | 92.2% | 91.00% |
| F1 Score | 91.5% | 90.00% |
| ROC AUC | 94.15% | 93.24% |

These numbers spell out high model capability in the correct detection of attacks across IoT networks, the result of model architecture and learning process optimizations. The training data points to the high adaptability of the model to the dataset used in training; the test data, on the other hand, offers practical proof of how this model will perform in real life.

In the next segment, we evaluate the proposed hybrid model, which incorporates CNN, GRU, and LSTM architectures, with other algorithms typically utilized in deep studying for attack detection. These algorithms consist of RNN, LSTM-RNN, GRU, and GRU-CNN. The goal of this contrast is to evaluate the relative overall performance of the hybrid model in opposition to different conventional procedures and decide the volume of development this hybrid combination can provide in phrases of detection accuracy and performance.

The contrast effects are displayed in the desk beneath, which incorporates key metrics along with accuracy, precision, consider, and F1 rating for each algorithm. This fact helps us gain a higher know-how of each model's abilities while dealing with complex and imbalanced facts.

Table 6: Simulation Results

| Algorithm | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Proposed Model | 93.24% | 89.00% | 91.00% | 90.00% |
| RNN | 89.50% | 85.00% | 88.00% | 86.50% |
| LSTM-RNN | 91.00% | 87.00% | 89.50% | 88.25% |
| GRU | 92.00% | 88.50% | 90.00% | 89.25% |
| GRU-CNN | 92.50% | 88.75% | 90.50% | 89.62% |

The analysis of the information in the assessment results desk suggests that the proposed hybrid version (CNN-GRU-LSTM) has efficiently outperformed different fashions below evaluation, consisting of RNN, LSTM-RNN, GRU, and GRU-CNN. This improvement in overall performance, in particular in precision and F1 score metrics, indicates that combining one of a kind deep getting to know architectures with unique parameter and characteristic optimization thru the PSO algorithm extensively enhances the version's potential to correctly and efficiently stumble on assaults in imbalanced and complicated environments. This analysis demonstrates that superior and hybrid strategies in constructing deep studying models can be tremendously powerful in addressing challenges in figuring out complicated records styles.

The following figure shows the confusion matrices for all of the models that are being compared to in this paper. The

reason for such charts is to get a broader assessment and analysis of the performance of the models in correctly and, wrongly, diagnosing the data classes.

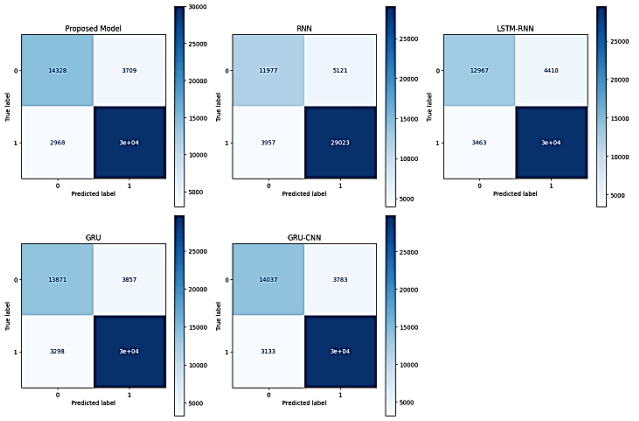


Fig. 1 confusion matrix

Using the confusion matrices, a complete understanding of the accuracy of the classification for all models, including the CNN-GRU-LSTM hybrid proposed in this work and five others, RNN, LSTM-RNN, GRU, and GRU-CNN is given. The performance metrics do suggest that the proposed model rightly identifies more number of samples correctly as indicated by the true positives and true negatives and is lower in error rates to the other models. This shows that the model performs well to identify between various classes of data with the least possible discrepancies as compared to RNN and LSTM-RNN which have provided nearly wrong readings for both the positive and negative samples. Furthermore, it is evident that the combined CNN-GRU-LSTM has the strength of each of the architectures and saves much less erroneous calculations and improves its generality. Comparatively, there are drawbacks related to simpler models which run into what are referred to as complex patterns of data and results in higher error rates. Indeed, this analysis emphasizes that it is possible to increase classification model accuracy and reliability by utilizing excellent hybrid combinations of the architectures described above, particularly when working with skewed or multimodal datasets.

Additionally, evaluating the hybrid model's overall performance with different fashions reveals that integrating layers with complementary talents, inclusive of GRU and LSTM layers mixed with CNN layers, complements the model's detection and discrimination capabilities. This integration improves the precise detection of touchy and essential statistics areas, in the end main to better standard model accuracy in actual-world situations. Therefore, evaluation strategies primarily based on a couple of metrics, which includes ROC AUC, are specifically vital in reading model performance in diverse check and schooling eventualities. These analyses provide a scientific foundation for better expertise and continuously optimizing deep studying fashions to evolve to actual facts and lay the basis for future improvements in detection and safety technology.

In this section of the research, we expose the limitations encountered in this study. Knowing the limitations would provide a more accurate rendering of the results and help future studies in enhancing these models.

### 5-1- Data Limitations:

- The facts used in this observe might not comprehensively cover all aspects of protection threats in IoT networks. Specifically, the restricted availability of datasets containing real and up to date assault statistics can have an effect on the algorithms' capability to train and test correctly. This obstacle is specifically full-size while the model needs to pick out new and rising assaults.

### 5-2- Computational Limitations:

- Implementing the hybrid algorithms and optimizations used in this research, mainly genetic and PSO algorithms, calls for excessive computational electricity and hardware resources. This can be difficult in environments with restrained resources. High computational complexity may also growth operational expenses and create boundaries for the extensive deployment and sensible software of these models in the industry.

These limitations impact the development and development of the proposed models and have to be addressed in destiny research thru progressive strategies and new technologies. Understanding these obstacles allows choice- makers and researchers expand more effective strategies for applying the effects of this take a look at in actual-international situations.

## 6- Conclusion

In this paper, we focused on the design and implementation of a hybrid CNN-GRU-LSTM model targeted at enhancing the security in IoT networks. The model integrates big data analytics with deep learning and PSO for a more robust and proactive mechanism against cyber threats. Much emphasis is given to the precise selection of hyperparameters through the PSO optimization process to increase the model's accuracy in attack detection.

Evaluations showed that at the very least, the proposed algorithm outperformed other state-of-the-art models like RNN, LSTM-RNN, GRU, and GRU-CNN. Specifically, created results of this comparison in metrics such as ROC-AUC, F1 Score, Recall, Precision, and Accuracy proved the effect of this hybrid approach. This model has advantages not only in theoretical power but also in practical applicability, and thus can hugely enhance IoT security in real-world scenarios.

This paper has illustrated that recent deep learning algorithms along with optimization algorithms could be one of the excellent solutions for solving the security issues of IoT. Considering these results, the organizations dealing with IoT Technologies can use this model in their defensive strategies and make the data and connected devices associated secure.

Future Research Recommendations:

- Hyperparameter Optimization: The hyperparameter optimization may be performed a whole lot deeper, and greater superior techniques of PSO may be used for similarly overall performance improvement.
- Scalability: Whether this algorithm scales to more complicated and larger IoT environments and at what level, in order that proposed answers are nonetheless powerful in larger dimensions.
- Field Deployment: Partner with industrial partners for the checking out of the fashions with the aid of actual-international deployments that generate critical feedback about the effectiveness and performance of the answers in real conditions.

This research is a sizable step in growing deep learning-primarily based protection answers for IoT networks and sets the level for destiny advancements in this area.

## References

[1] M. Haras and T. Skotnicki, "Thermoelectricity for IoT – A review," 2018. doi: 10.1016/j.nanoen.2018.10.013.

[2] A. Ullah, N. Javaid, O. Samuel, M. Imran, and M. Shoaib, "CNN and GRU based Deep Neural Network for Electricity Theft Detection to Secure Smart Grid," in 2020 International Wireless Communications and Mobile Computing, IWCMC 2020, 2020. doi: 10.1109/IWCMC48107.2020.9148314.

[3] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," Sensors, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[4] C. U. Om Kumar, S. Marappan, B. Murugeshan, and P. M. R. Beaulah, "Intrusion Detection Model for IoT Using Recurrent Kernel Convolutional Neural Network," Wirel Pers Commun, vol. 129, no. 2, 2023, doi: 10.1007/s11277-022-10155-9.

[5] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, no. 5, 2021, doi: 10.3390/pr9050834.

[6] A. Dushimimana, T. Tao, R. Kindong, and A. Nishyirimbere, "Bi-directional Recurrent Neural network for Intrusion Detection System (IDS) in the internet of things (IoT)," International Journal of Advanced Engineering Research and Science, vol. 7, no. 3, 2020, doi: 10.22161/ijaers.73.68.

[7] N. W. Khan et al., "A hybrid deep learning-based intrusion detection system for IoT networks," Mathematical Biosciences and Engineering, vol. 20, no. 8, 2023, doi: 10.3934/mbe.2023602.

[8] S. M. Jagannath, R. B. Mohite, M. K. Gupta, and O. S. Lamba, "Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems," Indian J Sci Technol, vol. 16, no. 9, pp. 640–647, May 2023, doi: 10.17485/IJST/v16i9.99.

[9] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks," in 2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018, 2018. doi: 10.1109/NETSOFT.2018.8460090.

[10] S. A. Alabady, F. Al-Turjman, and S. Din, "A Novel Security Model for Cooperative Virtual Networks in the IoT Era," Int J Parallel Program, vol. 48, no. 2, 2020, doi: 10.1007/s10766-018-0580-z.

[11] A. A. Alahmadi et al., "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," 2023. doi: 10.3390/electronics12143103.

[12] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," IEEE Signal Process Mag, vol. 35, no. 5, 2018, doi: 10.1109/MSP.2018.2825478.

[13] M. Jain, V. Saihjpal, N. Singh, and S. B. Singh, "An Overview of Variants and Advancements of PSO Algorithm," 2022. doi: 10.3390/app12178392.

[14] J. Fang, W. Liu, L. Chen, S. Lauria, A. Miron, and X. Liu, "A Survey of Algorithms, Applications and Trends for Particle Swarm Optimization," International Journal of Network Dynamics and Intelligence, 2023, doi: 10.53941/ijndi0201002.

[15] A. Aribisala, M. S. Khan, and G. Husari, "Feed-Forward Intrusion Detection and Classification on a Smart Grid Network," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022, 2022. doi: 10.1109/CCWC54503.2022.9720898.

[16] W. H. Lin, P. Wang, B. H. Wu, M. S. Jhou, K. M. Chao, and C. C. Lo, "Behaviorial-Based Network Flow Analyses for Anomaly Detection in Sequential Data Using Temporal Convolutional Networks," in Lecture Notes on Data Engineering and Communications Technologies, vol. 41, 2020. doi: 10.1007/978-3-030-34986-8_12.

[17] M. Chattopadhyay, "Modelling of intrusion detection system using artificial intelligence—evaluation of performance measures," Studies in Fuzziness and Soft Computing, vol. 319, 2015, doi: 10.1007/978-3-319-12883-2_11.