International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 3, Issue 1, January – February (2025)

RESEARCH ARTICLE

CDDI-IDS: DEEP LEARNING MODEL FOR CYBERATTACK DETECTION IN IOT DEVICE

Vinoth Rathinam [1, *], Valarmathi K [2], Ramathilagam Arunagiri [3]

[1] Associate Professor, Department of Electronics and Communication Engineering, P.S.R. Engineering College, Sivakasi, Tamil Nadu 626140, India
[2] Professor, Department Electronics and Communication Engineering, P.S.R. Engineering College, Sivakasi, Tamil Nadu 626140, India.
3 Professor, Department of Computer Science and Engineering, P.S.R. Engineering College, Sivakasi, Tamil Nadu 626140, India.
[*]*Corresponding e-mail: vinoth@psr.edu.in*

Abstract – The Internet of Things (IoT) has transformed modern technology by connecting smart gadgets. While these advancements provide unparalleled potential, they also pose complicated security issues. Deep Learning has shown potential for identifying and detecting cyberattacks on IoT devices. Intrusion Detection System (IDS) is critical for protecting sensitive data by detecting and mitigating suspicious activity in the IoT setting. To overcome these issues a novel Deep Learning-Based Cyber-attack detection in IOT device (CDDI-IDS) has been proposed in this paper, for effectively detecting and categorizing the types of attacks in IoT. The process starts with collecting data from IoT devices, which is then transferred through the pre-processing stage from the IOT device, which records network data and log files. The processed data is subsequently cleaned and normalized to reduce noise and improve model performance. Renyi Entropy is used for the feature extraction process to select the most important feature while minimizing noise. Dingo Optimization is used to tune hyperparameters, improving accuracy and efficiency. Finally, the trained model was classified using ConvBiGRU, which detects sequential patterns in time-series data as Normal, Probe, R2L, DoS, and U2R. This deep learning-based technique improves cyber threat detection accuracy, making it perfect for protecting IoT networks from hostile activity. Experiments on the KDDCup99 datasets demonstrate that intrusion detection system outperforms existing approaches and models. The CDDI-ID method achieves 99.23% accuracy, while the DNN, LSTM, CNN methods achieve 96.56%, 92.2%, and 94.5%, respectively.

Keywords *– Intrusion detection, Deep Learning, Dingo optimization, Internet of things, Renyi entropy.*

1. INTRODUCTION

IoT is a new technology concept characterized by a global network of connected electrical devices. Its primary purpose is to improve people's daily lives by automating routine tasks over the lifespan [1]. Security worries over the impact of assaults on linked devices have eased. Furthermore, the sensitivity of data available on IoT devices proved critical in locating methods for detecting and responding to these threats [2]. Because of its limitations, IoT is impotent against attacks and security concerns. Internet of Things has enormous promise for the development of sustainable communities [3]. Personal information may be gathered directly or indirectly by the Internet of Things. Localization, tracking, and customization privacy hazards may arise from the direct revelation of private data, such as identity, location, and sensitive information [4].

Internet of Things has enormous promise for the development of sustainable communities. Personal information may be gathered directly or indirectly by the Internet of Things [5]. Localization, tracking, and customization privacy hazards may arise from the direct revelation of private data, such as identity, location, and sensitive information [6]. IoT gadgets include mobile phones, video cameras, industrial devices, and sensors that are all connected to the Internet. However, IoT networks create significant data flow among networked devices, making them prime targets for cyber threats and assaults. Because of inherent vulnerabilities, attackers frequently exploit these flaws using sophisticated ways [7].

IoT gadgets include Internet-connected mobile phones, video cameras, industrial devices, and sensors. However, IoT networks allow for massive data flow between networked devices, making them excellent targets for cyber threats and attacks. Because of the inherent vulnerabilities, attackers regularly exploit them in clever ways [8]. Malware and other network assaults attempt to compromise the confidentiality, integrity, and availability of the computing device or network attached. [9]. In the detection stage, acquired data is analyzed using signature-based and anomaly-based algorithms to identify malicious network activity [10]. The proposed CDDI-IDS framework contribution are as follows:

- Initially, the process starts with collecting data from IoT devices and pre-processed data, including data cleaning, normalization, to remove irrelevant data.
- The CDDI-IDS method utilizes a Renyi Entropy to extract the relevant features.
- CDDI-IDS approach utilizes a CovBiGRU to classify intrusions like Normal, DoS, R2L, U2R,

and Probe. The suggested technique efficiency is assessed utilizing accuracy, precision, recall, f1score, and MSE.

- Finally, classified intrusion is in Hyper Parameter Tuning process by using Dingo Optimization to select most relevant features accurately.

The remaining portion of this research is as follows: Literature survey is summarized in Section 2, and Section 3 details the suggested framework. Section 4 details results and discussion. Future work and conclusion are included in Section 5.

2. LITERATURE SURVEY

In 2020, Abu Al-Haida, Q. and Zein-Sabatto, [11] proposed IoT-IDCS-CNN takes use of high-performance computing, which leverages the resilient CUDA-based Nvidia GPUs, as well as parallel processing, which employs high-speed Intel CPUs with I9 cores. This research involved the development, verification, integration, and validation of all subsystems. To assess the proposed system, NSL-KDD dataset, which contains all of the important attacks in IoT computing.

In 2020, Al-Abassi, A., et al., [12] suggested a deep learning model for creating balanced and unbalanced datasets. The newly developed representations are applied to an ensemble deep learning attack detection model specifically created for the ICS context. The suggested attack detection technique uses DNN and DT classifiers to detect cyberattacks in novel forms. The performance suggested model assessed using ten-fold cross-validation on two real-world ICS datasets. The method outperforms both conventional classifiers like RF, DNN, AdaBoost, as well as freshly released models in the literature. The recommended strategy is comprehensive and easily implementable in current ICS systems.

In 2022, Tsimenidis, S., et al., [13] proposed for IoT intrusion detection. In a detailed, structured review of how deep learning has been implemented for IoT cybersecurity, solutions were classed by model, as well as their distinctive contributions to the creation of efficient IoT intrusion detection systems. IoT is a desirable target for fraudsters, making cybersecurity a primary issue for the IoT ecosystem. Although cybersecurity has been studied for decades, large-scale IoT architecture and emergence of new threats have rendered traditional tactics ineffective. Deep learning has the potential to provide cutting-edge solutions for IoT intrusion detection due to its data-driven, anomaly-based methodology and ability to detect upcoming assaults.

In 2022, Otoum, Y., Liu, D. and Nayak, A., [14] identified security threats in IoT contexts, a deep learning-based intrusion detection system was presented. Although there are several IDSs available in the literature, their ineffective feature learning and data set management greatly impact the assault detection accuracy. The stacked-deep polynomial network and SMO techniques are combined in our suggested module to provide optimal detection identification. While SDPN categorizes data as normal or anomalous, SMO selects the best characteristics from datasets. DL-IDS may identify a variety of anomalies, including DoS, U2R, probing, and remote-to-local assaults.

In 2023, Sharma, B., et al., [15] developed IoT networks from diverse assaults, an effective and useful intrusion detection system might be a workable answer. A filter-based feature selection DNN model, in which highly correlated features are eliminated, was given. Furthermore, the model is tweaked using a variety of parameters and hyperparameters. The UNSW-NB15 dataset, which contains assault classes, was used for this purpose. Since a large number of devices in an IoT ecosystem are connected over the internet, IoT networks are more vulnerable to different types of cyberattacks; as a result, network security, user privacy and are crucial considerations when implementing IoT systems.

In 2024 Hizal, S., et al., [16] proposed IDS powered by deep learning models, to improve threat detection and mitigation. The cornerstone framework is built on gathering and preparing a broad dataset of IoT network traffic data, which includes both regular and aberrant activity. The dataset's consistency for future research by performing preprocessing activities such as data cleansing, standardization, and appropriate formatting. The cutting-edge deep-learning models to deliver accurate and efficient IDS. Specifically discuss DNN, LSTM, CNN.

In 2024, Nandanwar, H. and Katarya, R., [17] proposed robust deep learning model called AttackNet for detecting and classifying various botnet attacks in IIoT using an adaptive CNN-GRU model. The model are completely evaluated using the most recent dataset and conventional performance evaluation indicators, confirming its ability to safeguard IIoT networks. In terms of accurately identifying and categorizing botnet assaults, the model outperforms state-of-the-art IIoT anomaly detection methods based on real-time IoT device datasets. Multi-variant persistent and sophisticated bot attacks can have catastrophic effects on linked IIoT, and identifying them is a crucial and difficult undertaking.

From the above literature survey, several shortcomings are faced by existing methods such as potentially impacting system performance, security, scalability, and efficiency. This research introduces a novel method called CDDI-IDS, which will be covered in more depth in the next part to overcome these problems.

3. PROPOSED METHODOLOGY

In this study, a novel CDDI-IDS model approach is to detect cyber threats for intrusion detection in IOT devices. The process begins with data collection from IoT devices, which is then passed through the pre-processing stage from IOT device to capture network traffic and system logs. Then the collected data is pre-processed with cleaning and normalization to remove noise and standardize for better model performance. For feature extraction, the Renyi Entropy is used to select the meaningful feature while reducing the noise. Hyperparameter tuning Dingo Optimization is applied, optimizing parameters for better accuracy and efficiency. Finally, the trained model classified using ConvBiGRU model for capturing sequential patterns

in time-series data as Normal, Probe, R2L, DoS, U2R. This deep learning-based technique improves cyber threat detection accuracy, making it extremely useful for protecting IoT networks from unwanted activity. Figure 1 shows the overall workflow of the suggested CDDI-IDS methodology.

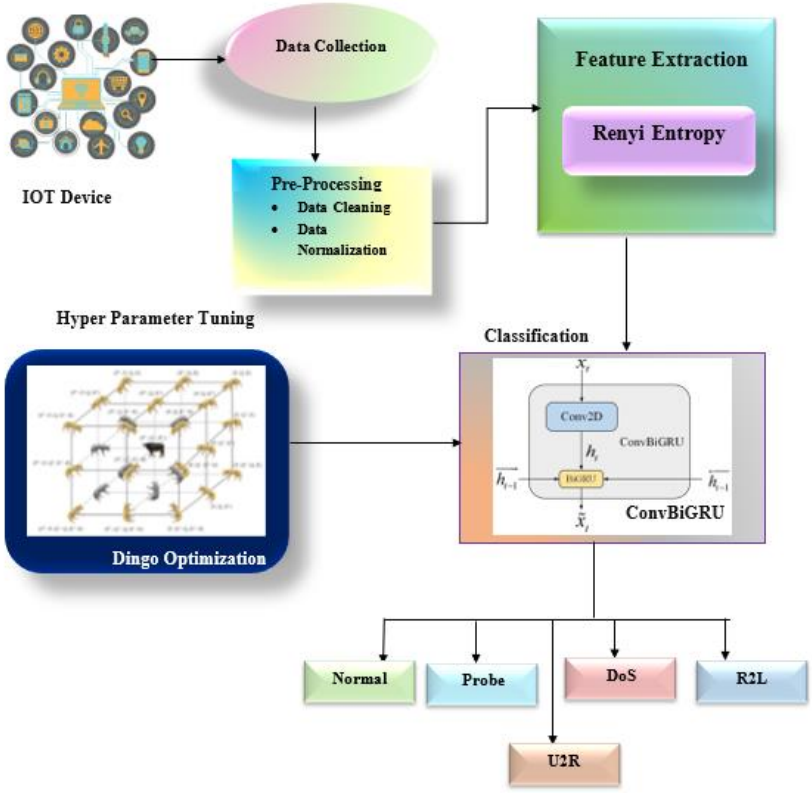


Figure 1. CDDI-IDS Framework

3.1 Data Collection

Data collection involves acquiring data from IoT devices, sensors, and network logs to monitor activities and detect potential threats. This data may include network traffic, device behavior, system logs, or environmental parameters, which are crucial for identifying anomalies and security risks.

3.2 Data Preprocessing

Preprocessing converts incoming data into a usable format by removing extraneous information. The model's accuracy and efficiency can only be improved by altering and preparing data to suit the learning process. The preparation phase includes the following tasks:

Data Cleaning: Data cleaning is fixing errors and identifying irregularities in data to improve its quality. This method includes dealing with null values using techniques like median, interpolation, and means, as well as dealing with outliers by deleting or changing them into a more appropriate range.

Z-Score Normalization

A z-score's value shows deviation from the mean in standard deviations. Z-score of 0 indicates the mean. When the z-score is positive, the raw score exceeds the mean average. A preprocessing technique called normalization breaks down numerical properties and transforms them into a certain range. There are various methods for normalizing data, including decimal scaling, z-score, and min-max.

Equation 1 illustrates how Z-score normalization maps a previously unknown range of vi values from attribute E.

$$v' = \frac{v_i - E_i}{std(E)} \quad (1)$$

v' represents the normalized value. v denotes the value to be normalized in the attribute. Ei refers to the attribute's mean value, while std(E) represents its standard deviation.

3.3 Feature Extraction via Renyi Entropy

Rényi entropy used as a feature extraction technique to enhance the learning process by capturing significant patterns and reducing irrelevant information in input data. The order parameter (α) in Rényi entropy controls the sensitivity to frequent or rare events, allowing the extraction of features that highlight different levels of data variability.

The detection of unexpected network activities in cybersecurity and IoT applications, making deep learning models more effective at detecting risk. By strengthening models and improving classification accuracy and overall performance in complex data-driven tasks, Renyi Entropy is included into deep learning frameworks.

The limit case of the Shannon entropy, while the Rényi entropy is a measure of information of order α. It can be described as:

$$ReEn = \frac{1}{1-\propto}\log\left(\sum_i^N (px_i)^{\propto}, \quad \propto \geq 0, \propto \neq 1 \right. \tag{2}$$

Where $\sum_{i=1}^{k} p_i = 1 \; and \; lim_{\propto \to 1} R_{\propto}(C) = H(C)$

Mutual information can be expressed as follows using Rényi entropy of order α ϵ (0, 1):

$$I_R(C; A_i) = R_{\propto}(C) - R_{\propto}(C|A_i) \tag{3}$$

3.4 Classification Via ConvBiGRU

ConvBiGRU is a powerful deep learning architecture for classification problems, particularly those involving sequential and spatial data, such as text, speech, and time-series analysis. It uses Convolutional Neural Networks (CNNs) for efficient feature extraction and Bidirectional Gated Recurrent Units (BiGRU) for sequential modeling. The CNN layers detect local patterns and spatial dependencies in the input, such as phonemes in speech or word n-grams in text, but the BiGRU layers handle sequential dependencies in both forward and backward directions, thereby enhancing context comprehension.

To accomplish this, the ConvBiGRU model, depicted in Figure 2, performs the fusion of information from multiple slices along with their spatial correlation.

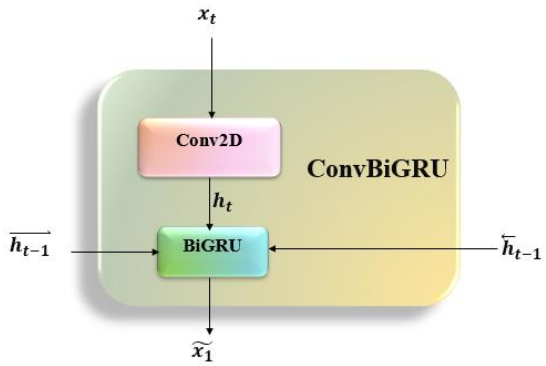


Figure 2. ConvBiGRU structure

The GRU cell equations are used to determine forward and backward hidden states at each time step (t). The gate (z) decides how much past knowledge to retain, when the reset gate (r) controls how much past information is to forget. These gates are formed as follows:

$$z_t = \sigma(W_z F_t + U_z h_{t-1} + b_z) \tag{12}$$

$$r_t = \sigma(W_r F_t + U_r h_{t-1} + b_r) \tag{13}$$

The candidate hidden $\widetilde{h_t}$Computed as:

$$\widetilde{h_t} = \tanh\left(W_h F_t + U_h(r_t \odot h_{t-1}) + b_n\right) \tag{14}$$

At time t, the final concealed state is modified as follows:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \widetilde{h_t} \tag{15}$$

Because BiGRU process the sequence in both directions, each time step's final representation is produced by concatenating the forward and backward hidden states:

$$H_t = [h_t^f; h_t^b] \tag{16}$$

For classification, the BiGRU sequence's final hidden state is sent to a fully linked layer:

$$Y = Softmax(W_o H + b_o) \tag{17}$$

Softmax converts the final outputs into probability distributions across classes. The model then allocates the input sequence to the class with the highest probability, proving useful for time-series classification, intrusion detection, speech recognition, and anomaly detection. For sentiment analysis with an optimization algorithm, ConvBiGRU deep learning classifier shown in Figure 3

3.5 Hyper Parameter Tuning

Dingo Optimization (IDO)

The optimization model of Improved Dingo Optimization (IDO) is designed for hyperparameter tuning to optimize data and provide relevant features. Reaching optimal Real-world system solutions is quite complicated due to the presence of more than one optimal solution. The persecution, scavenging, collective attack, and survival are enhanced by (4)-(6).

$$\beta = (\mathrm{BF} - \mathrm{WF}) \tag{4}$$

$$\mathrm{Y} = \frac{\mathrm{mean(D(F-WF))}}{\mathrm{mean(D(F-BF))}} \tag{5}$$

$$\mathrm{UB} = \beta \times \left(\frac{\mathrm{q}}{\mathrm{Y}}\right) \tag{6}$$

Here, the terms BF and WF represent the best and worst objective function respectively. F stands for fitness, D represents distance, Y and q are in general, and UB is an arbitrary value falling between 0 and 1.

Step 1 - Group Attack: Dingoes hunt in groups, using their tracking skills to surround prey. This is represented by an equation.

$$\overrightarrow{\mathrm{D_b}}(\mathrm{l}+1) = \propto_1 \sum_{\mathrm{v}=1}^{\mathrm{ui}} \left(\frac{\overrightarrow{\emptyset \mathrm{k(d)}} - \mathrm{d}\vec{\mathrm{p}}(\mathrm{l})}{\mathrm{ui}}\right) - \vec{\mathrm{d}} \times (\mathrm{l}) \tag{7}$$

$\overrightarrow{\mathrm{D_b}}(\mathrm{l}+1)$ represents the position of the feature, U_iIs a randomly selected number, dp $\vec{}$ represents the best iteration

constructed utilizing the preceding iteration, d $\vec{}\times$(z) tends the search agent, ∅k(d) is the sub-set provided for all search agents and ∝_1 is an arbitrarily generated number that is equally produced and displayed in a range of [−2, 2] and which has been upgraded in Equation (7). Step 2 - Persecution: Dingoes often pursue small prey until they catch them within their grasp. This behavior is illustrated in equation (5).

$$\vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l}+1) = \vec{\mathrm{d}} \times (\mathrm{l}) + \propto_1 + \mathrm{f}^{\propto_2} \times (\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l}) - \vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l})) \tag{8}$$

Here, the term $\vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l}+1)$ denotes a dingo movement within the search engine $\vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l})$The derived random variable falls within [−1, 1] is represented as $\propto_2$, an arbitrary number q_1 is updated in Equation (8) and $\vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l})$ represents the search agent for the qThe interval.

Step 3 - Scavenger: Dingoes' scavenging features are regarded as an action when they find their meal and this behaviour is provided in equation (9).

$$\vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l}+1) = \frac{1}{2}[\mathrm{f}^{\propto_2} \times \vec{\mathrm{d}}_{\mathrm{q}_1}(\mathrm{l}) - (-1)^{\sigma} \times \vec{\mathrm{d}}_{\mathrm{p}}(\mathrm{l})] \tag{9}$$

The binary number, represented by the symbol σ, is produced spontaneously

Step 4: The dingo's survival rate is given in Equation (10).

$$\text{surv(D)} = \frac{\text{BF}-\text{F(D)}}{\text{BF}-\text{WF}} \quad (10)$$

In the current generation, the least fitness function is represented as WF and BF represents the highest level of fitness. Fs(D) is the fitness value provided for D_{th} Search features and also Equation (11) determines the minimal survival rate.

$$\vec{d}_p(l+1) = \vec{d} \times (l) + \frac{1}{2}[\vec{d}_{q_1}(l) - (-1)^{\sigma} \times \vec{d}_{q_2}(l)] \quad (11)$$

The chosen search agent for the numerical value q_1 and q_2 is stated as $\vec{d}_{q_1}(l)$ and $\vec{d}_{q_2}(l)$, correspondingly, updates the random integers. Here, the lowest survival rate is indicated as $\vec{d}_p(l)$. Figure 3 depicts the positions of neighboring dingoes in two dimensions.

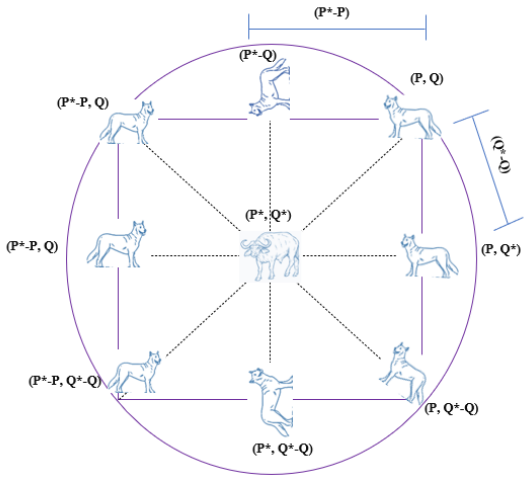


Figure 3. 2D Position vectors of dingoes

4. RESULTS AND DISCUSSIONS

The suggested CDDI-IDS method performance is compared with the existing method regarding recall, precision, accuracy, f1score, MSE. The efficacy of the proposed method for intrusion detection is measured using the publicly available large datasets, KDDCUP 1999

4.1 Dataset Description

The most popular and widely used intrusion detection datasets are the KDD 1999 datasets, which were created during the KDD Cup competition. This dataset is based on the 4 million records in the DARPA 1998 dataset. The KDD 1999 datasets, normal and 22 assaults, are separated into five main parts. Regular, DoS, R2L, probing, and U2R attacks are among the several varieties. 41 attributes include traffic, content, and basic operational components

4.2 Performance Analysis

Performance metrics like accuracy, precision, F1-score, MSE, recall is used to calculate the suggested method approach. Basic parameters like FalP, TruN, FalN, and TruP can be used to create these evaluation metrics.

Accuracy: An essential metric to gauge accurate sensor readings. Because it is proportional to the total number of values, statistical accuracy increases in balanced sensor nodes, where FalP and FalN are almost equal.

$$\text{Accuracy} = \frac{\text{TrP}+\text{TrN}}{\text{FalN}+\text{TrP}+\text{FalP}+\text{TrN}} \quad (10)$$

Precision: It is expressed as a proportion of accurately predicted positive among all positive predictions.

$$\text{Precision} = \frac{\text{TrP}}{\text{TrP}+\text{FalN}} \quad (11)$$

Recall: It is a positive comment ratio that was correctly anticipated based on all actual observations made in class.

$$\text{Recall} = \frac{\text{TrP}}{\text{TrP}+\text{FalN}} \quad (12)$$

F1 score: Precision and recall are weighted and averaged. Both FalN and FalP are taken into consideration in this score.

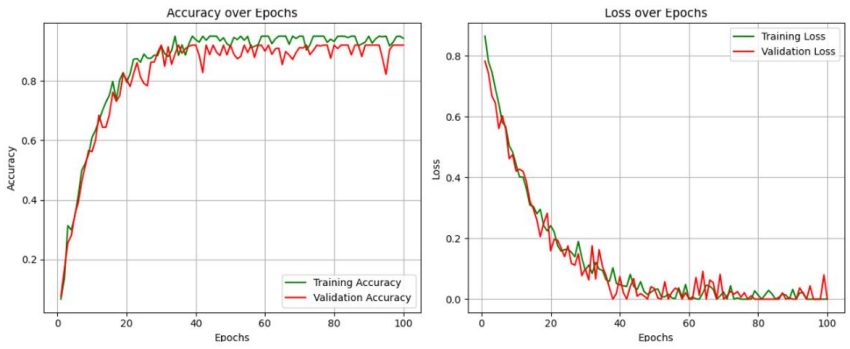
$$\text{F1 score} = 2 \times \frac{\text{PR.RC}}{\text{PR}+\text{RC}} \quad (13)$$

Mean Squared Error (MSE): The MSE is used to analyze efficiency throughout the Epoch Process. MSE is defined as follows:

$$\text{MSE} = \frac{1}{M}\sum_{l=1}^{M}(q_{\text{input}} - q_{\text{output}})^2 \quad (14)$$

Where, q_{input} is the initial input, q_{output} Is the output, M is the number of sensor nodes.

Attack is defined as $\propto$_SN when the SN wrongly recognizes the normal or attack, where p is the total number of accessible sensor nodes.



(a) (b)

Figure 4. Accuracy and Loss curve of KDDCUP99 dataset

The classification validation and testing are illustrated through accuracy and loss plots of proposed intrusion detection methods in Figures 4(a) and 4(b). These charts show the model's performance and demonstrate its effectiveness in identifying intrusions. Furthermore, low loss values indicate successful learning with minimal overfitting throughout the training process. Performance Evaluation of proposed model is shown in Figure 5.

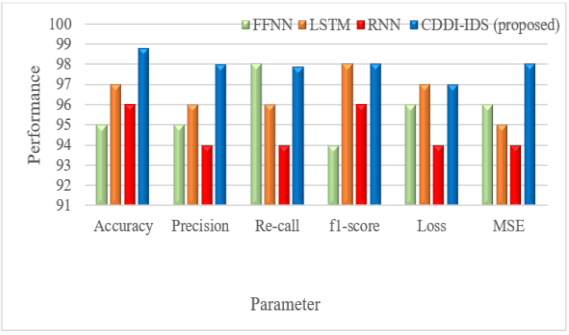


Figure 5. Performance Evaluation of CDDI-IDS Model

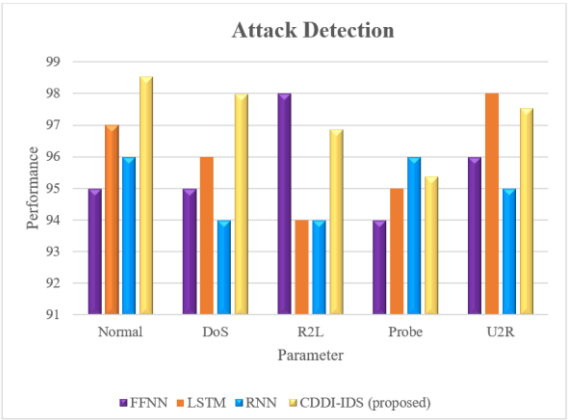


Figure 6. Attack detection of Proposed Method

Performance assessment of the proposed system using a variety of techniques relating to attack detection rate. Figure 6 illustrates Attack Detection Rate (ADR) for various methods, comparing Normal, Dos, R2L, U2R, Probe, and the Attack detection performance. The proposed range is 98.54% detection rate, while existing methods achieved only 93.85% for FFNN, 96.8% for LSTM, 97.12% for RandNN.

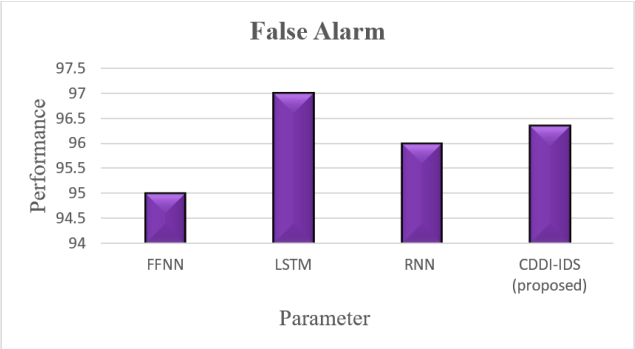


Figure 7. False alarm rate for Proposed Method

Figure 7 represents the false alarm rate 96.35% for various IDS across the false detection rates. Overall, the proposed CDDI-IDS demonstrates superior effectiveness in minimizing false alarms compared to the other methods.

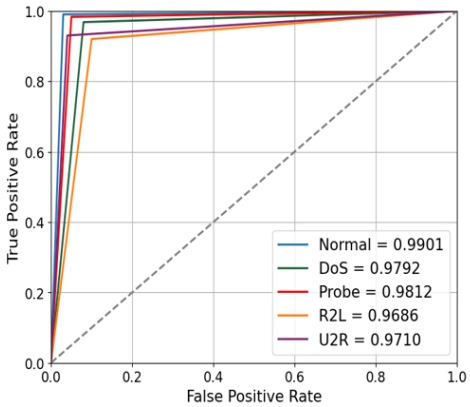


Figure 8. ROC curve of KDDCUP99

Figures 8 show the ROC of normal, u2r, dos, r2l, and probe classification results using KDDCUP99. The suggested CDDI-IDS achieved an AUC of 0.9901 for normal, 0.9792 DoS, 0.9812 Probe, 0.9686 R2L and 0.9710 U2R cases that were established by FPR and TPR parameters for the KDDCUP99 dataset.

5. CONCLUSION

In this study, a novel CDDI-IDS Framework to detect and classify cyber-attacks. The process begins with preprocessing from the IOT device, which captures network

traffic and log files. The processed data is then cleaned and normalized to remove noise and improve model performance. Renyi Entropy is used for feature extraction to choose the most significant feature while decreasing noise. Dingo Optimization is used for hyperparameter tuning, which improves accuracy and efficiency. Finally, the trained model was classified using ConvBiGRU, which captures sequential patterns in time-series data as Normal, Probe, R2L, DoS, U2R. This deep learning-based technology improves cyber threat detection accuracy, making it ideal for defending IoT networks from malicious activities. Experiments on the KDD Cup99 datasets show that the proposed intrusion detection system surpasses the existing methods models. The accuracy approach for the CDDI-ID method is 99.23% and DNN, LSTM, CNN methods achieve a low accuracy of 96.56%, 92.2%, and 94.5% respectively. The suggested technique efficiency is assessed utilizing accuracy, precision, recall, f1score, and MSE. Future work will further enhance the scalability and adaptability of the CDDI-IDS system to handle growing intrusion patterns and larger, more diverse datasets.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] N. Islam, F. Farhin, I. Sultana, M.S. Kaiser, M.S. Rahman, M. Mahmud, A.S.M.S. Hosen, and G.H. Cho, "Towards machine learning based intrusion detection in IoT networks", *Comput. Mater. Contin,* vol. 69, no. 2, pp. 1801-1821, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S.A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model", *Computers and Electrical Engineering*, vol. 99, pp. 107810, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity", *Computers & Security*, vol. 118, pp. 102748, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] M. Ge, N.F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly. "Towards a deep learning-driven intrusion detection approach for Internet of Things", *Computer Networks*, vol. 186, pp. 107784, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] M.A. Alsoufi, S. Razak, M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, and M. Nasser. "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review", *Applied sciences*, vol. 11, no. 18, pp. 8383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] A. Amouri, V.T. Alaparthy, and S.D. Morgera. "A machine learning based intrusion detection system for mobile Internet of Things", *Sensors*, vol. 20, no. 2, pp. 461, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadili, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks", *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] M. Roopak, G.Y. Tian, and J. Chambers, January. An intrusion detection system against DDoS attacks in IoT networks. In 2020 10th annual computing and communication workshop and conference (CCWC), pp. 0562-0567, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Y.K. Saheed, and M.O. Arowolo, "Efficient cyber-attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms", *IEEE Access*, vol. 9, pp.161546-161554, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] J. Shareena, A. Ramdas, and H. AP. "Intrusion detection system for iot botnet attacks using deep learning", *SN Computer Science*, vol. 2, no. 3, pp.1-8, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Q. Abu Al-Haija, and S. Zein-Sabatto. "An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks", *Electronics*, vol. 9, no. 12, pp. 2152, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R.M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system", *IEEE Access*, vol. 8, pp. 83965-83973, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. Tsimenidis, T. Lagkas, and K. Rantos. "Deep learning in IoT intrusion detection", *Journal of network and systems management*, vol. 30, no. 1, pp. 8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT", *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p.e 3803, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique", *Computers and Electrical Engineering*, vol. 107, pp. 108626, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security", *Internet of Things*, vol. 28, pp. 101336, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] H. Nandanwar, and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IOT environment", *Expert Systems with Applications*, vol. 249, pp. 123808, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Vinoth Rathinam is currently working as Associate Professor in the Department of Electronics and Communication Engineering at P.S.R. Engineering College, Sivakasi, Tamil Nadu, India. He received his Bachelors of Engineering–Electronics and Communication Engineering from Mohamed Sathak Engineering College and Master of Engineering in VLSI Design under Anna University in the year 2007 and 2009 respectively. He received his Ph.D. in Information and Communication Engineering under Anna University in the year 2017. His area

of interest includes image processing, signal processing, and VLSI design. He has more than 15 years of professional experience in Engineering Colleges. He has published more than 25 papers in reputed journals/conferences. He has been granted 4 patents and published 7 patents. He has received grant of Rs.6lakhs from AICTE, Niral Thiruvizha Naan Mudhalvan etc.

Valarmathi K is currently working as a Professor in the Department of Electronics and Communication Engineering at P.S.R. Engineering College, Sivakasi, Tamil Nadu, India. She is having 25 years of teaching experience. She has published 46 papers in peer reviewed international journals and presented 84 papers in various national and international conferences. She has received best paper award for her paper in the International Conference on VLSI communication and Instrumentation (ICVCI 2011). Her research interests are System identification, Image processing, soft computing, Wireless networks, Cloud computing and Machine Learning. She is the reviewer in various peer reviewed journal of Elsevier, Springer, Taylor and Francis, IEEE, and Wiley publishers. She has been granted 5 patents and has published 16 patents. She is the recognized supervisor of Anna University, Chennai. 13 PhD scholars has been awarded under her guidance and 8 scholars are pursuing PhD.

Ramathilagam Arunagiri is currently working as a Professor in the Department of Computer Science and Engineering at P.S.R. Engineering College, Sivakasi, Tamil Nadu, India. She has 21 years of teaching experience. She completed her Ph.D. in Information and Communication Engineering from Anna University in the year 2018. She obtained her M.E. Computer Science, Engineering in the year 2004, B.E. Computer Science, and Engineering in the year 1999 from Arulmigu Kalasalingam College of Engineering, Krishnankovil. She has published 15 papers in reputed international/national journals and presented 20 papers in National and International conferences. Her research interests are computer network, security, cloud computing, big data analytics, machine learning, and data science.

Arrived: 19.01.2025
Accepted: 25.02.2025