Trust Based Detection Of Rank Attack In Internet Of Things

Sonika[1], Meenu Vijarania[2], Vivek Kumar[3]
[1]PhD Scholar,K R Mangalam University, Gurugram, India
[2]K R Mangalam University, Gurugram, India
[3]Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India
sonikabhaskar241113@gmail.com

Abstract. *The Internet of Things (IoT) transforms everyday objects into smarter devices using technologies such as sensor networks. The routing Protocol for Lossy and Low-Power Networks (RPL) is a key protocol suitable for IoT environments, which often consists of devices with limited processing power, memory, and networking capabilities. Recent research has focused on developing IDS approaches that are more suitable for the IoT. In recent studies, machine learning has been used for feature selection in the IoT dataset, which helps to reduce the dimensions of the features and improve the detection accuracy. In some studies, deep learning methods have been used to handle large amounts of data and provide real-time analyses. Transfer learning has also evolved to adapt to IoT threats. This paper presents a novel approach for identifying intrusions in IoT networks. A hybrid approach using deep learning methods that combine trust-based parameters to enhance the early detection of known and unknown attacks in IoT traffic.*

Keywords: *Internet of Things, RPL, Rank Attack, Artificial Neural Network*

1 INTRODUCTION

With rapid changes in the IoT landscape, security has become increasingly important. Among the malicious threats to IoT systems are rank attacks. In rank attacks, hackers manipulate rankings to interfere with operations or steal data. The descriptive analysis of methods for detecting rank attacks in IoT devices explores the common vulnerabilities that make these devices susceptible to such attacks and delves into the impacts that rank attacks can have on IoT systems. For the detection of rank attacks on IoT devices, a multifaceted approach is required: monitoring the patterns of network traffic, data transmission rate anomalies, and implementing anomaly detection algorithms (Alsukayti and Alreshoodi 2023; Anitha and Arockiam 2019; Yavuz et al. 2018).

By monitoring interactions with IoT devices, network usage patterns such as an abrupt increase in data transmission can be viewed as a potential sign of a rank attack. Furthermore, advanced anomaly detection algorithms can alert users to normal device behavior, enabling them to mitigate the impact of such attacks by intervening in a timely manner.

The lack of secure authentication measures, insufficient encryption protocols, and insecurity in firmware and software updates make IoT devices an appealing target for rank attacks. Low-grade authentication control systems allow adversaries to access IoT devices and perform undesired manipulations such as changing the ranking of the devices and other turn-off functionalities. Additionally, weak ciphering techniques applied to device-to-device communication links provide easier interception and modification of the data being transferred, increasing the susceptibility to rank attacks. In addition, providing possibilities for attackers to penetrate the overall security of IoT environments is a weakness associated with firmware and software updates.

Consequently, these types of attacks can seriously disrupt the provision of service availability in IoT networks, compromise sensitive data, and cause loss of device performance as well as reliability. In this sense, there is an alteration of the normal functioning of IoT devices and persistent disruption of the critical services that these devices are meant to provide. In addition, the loss of Privacy or Intellectual Property can stem from the loss of sensitive data that are kept or sent by these IoT devices. Finally, the disruption of rank attacks on the performance and reliability of devices can affect the level of acceptability and ease of use of IoT, which threatens the sustainability of the systems. default passwords and badly designed communication channels open IoT devices to these attacks, together with unencrypted communication and security issues. As a result, both IoT devices and users must understand these threats and take appropriate measures in the form of secure security protocols to counter them.

To decrease the possibility of scarce resources being compromised and real-time detection of intrusion, the proposed R-Trust model is developed using a lightweight, high-level approach that comprises several phases, starting with data preprocessing (Alsukayti and Alreshoodi 2023). In addition, the features were normalized using min–max scaling to remove the worst overfitting that occurred because of training samples having fewer data, and then key features were selected. To ensure the survival of the service, the best runtime for the training accuracy was achieved through binary classification. Traditional IDSs that employ machine learning are not well equipped to deal with the specific challenges presented by IoT traffic because of the high dimensionality of data and the diverse nature of IoT devices (Zahra et al. 2022). These innovative approaches aim to create IDS solutions that are lightweight, efficient, and capable of detecting a wide range of attacks specifically tailored for the IoT ecosystem. This is an ongoing field of research, as the dynamic and diverse nature of IoT devices continues to present new challenges for security (Al-Amiedy et al. 2022). This study aims to validate the effectiveness of the IRAD dataset proposed by Yavuz et al. (2018) for classifying different types of attacks and validating the efficiency of the proposed hybrid IDS model. The classification of known and unknown attacks with the help of the proposed IDS model would be greatly beneficial to IoT networks in enhancing security because such networks are widely integrated into contemporary infrastructure.

The key contributions of this study can be summarized as follows:

The idea is to use the IRAD dataset for building and implementing an IDS that meets protocol requirements for IoT rather than other datasets where there are certain problems encountered in the process of collection over a traditional network.

- A trust factor for building contextual information creates an efficient detection model.
- Developing an efficient lightweight IDS model for IoT networks.
- To compare the performance of the proposed models against that of existing approaches

The following section provides an overview of the RPL protocol in a DODAG network. Section 3 discusses work on deep learning and intrusion detection systems (IDSs) regarding routing attacks in the RPL protocol.

The implementation phases, preprocessing data, and framework architectural sequence of the R-Trust model are covered in Section 4. Section 5 presents the findings of the analysis and evaluation and classifies the data by contrasting the R-Trust model with recent studies.

2 RPL Protocol

The Routing Protocol for Low-Power and Lossy Networks is designed as routing protocol designed for IoT networks, which are typically characterized as low-power and lossy in nature. RPL is intended for heterogeneous traffic networks, such as those in IoT, where devices often have limited power, memory, and processing capabilities. It is based on the IEEE 802.15.4 standard and allows both many-to-one and one-to-one communication (Han et al. In 2022 (Nayak et al. 2021). The RPL uses a tree-like structure called the destination-oriented directed acyclic graph (DODAG), which has a root node and a sink node that is rooted towards a node. The topology of the network is determined by an Objective Function that defines the best-optimized route among sensor devices based on their number (Alsulaiman and Al-Ahmadi 2021). RPL defines two modes of operation: the storing mode, which copies the entire routing table to all nodes, and the non-storing mode, which copies a list of default routes from parents to border routers.

DODAG, a Destination Oriented Directed Acyclic Graph, is a fundamental concept in the Routing Protocol for Low-Power and Lossy Networks (RPL), which is used in IoT networks (Saba et al. 2022). There are no cycles in a DAG-directed graph. Nodes in an RPL network self-organize into a DODAG based on an Objective Function (OF), which determines the best path through the network based on certain criteria such as link quality, hop count, or energy consumption (Saba et al. 2022; Saba et al. 2022; Sawafi et al. 2023). Each node in a DODAG is assigned a rank based on its distance from its root.

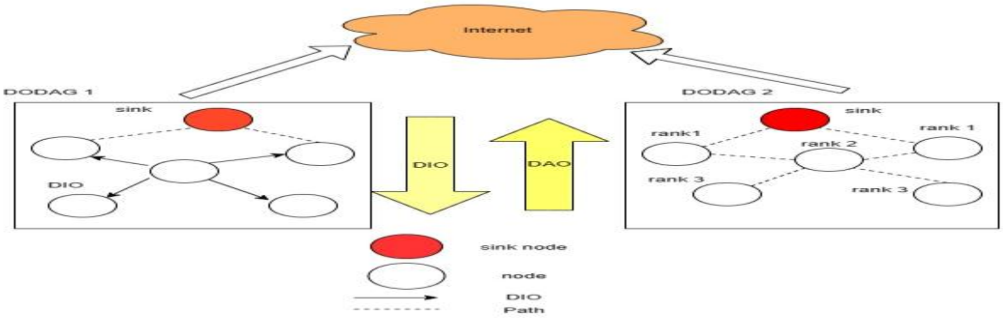


Fig. 1. RPL DODAG Structure

The rank increases as one moves away from the root, thereby ensuring a loop-free topology (Mohammadazadeh et al. 2022). Nodes select one or more parent nodes with a lower rank and provide a path towards the root. The preferred parent, or primary next hop for traffic heading towards the root, is usually one of these parents.

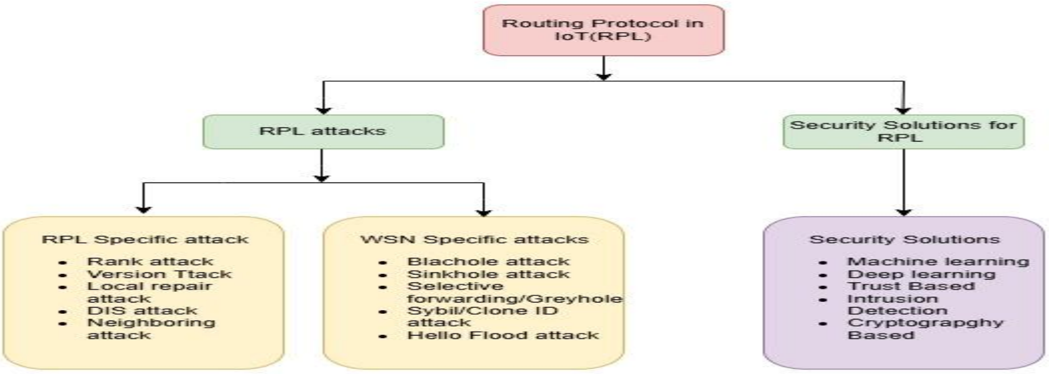
As shown in Figure 1, the DODAG structure allows for efficient routing in low-power and lossy networks by ensuring that all paths are oriented towards a common destination, minimizing the number of hops, and optimizing the use of limited resources.

2.1RPL Attacks

Many attacks can change the routing properties and parameters of an IoT network. Some attacks are WSN inherited, and some are RPL specific attacks. A rank attack is a more disruptive attack that affects the routing properties of the network. In this research rank attacks are considered as being more disruptive in nature.

2.2.1 Rank Attacks

The principal characteristic of RPL is the rank. It facilitates efficient and suitable routing mechanisms. Rank is responsible for monitoring control overhead, optimizing network topologies, and preventing the formation of loops. An assault on the rank property significantly impacts RPL's overall functionality and routing architecture. RPL lacks a mechanism to regulate node behavior, thereby increasing the potential for the emergence of rank-related attacks. The node selects a preferred parent based on the objective function, and its rank value is determined as disseminated by DIO messages within RPL routing. In the context of the DODAG, the rank ascends in the downward direction, specifically from the root to the leaf node. A rank attack occurs when an adversary manipulates the rank values.



Routing Protocol in IoT(RPL)

RPL attacks

Security Solutions for RPL

RPL Specific attack
- Rank attack
- Version Ttack
- Local repair attack
- DIS attack
- Neighboring attack

WSN Specific attacks
- Blachole attack
- Sinkhole attack
- Selective forwarding/Greyhole
- Sybil/Clone ID attack
- Hello Flood attack

Security Solutions
- Machine learning
- Deep learning
- Trust Based
- Intrusion Detection
- Cryptograpghy Based

Fig. 1. An overview of RPL and Security solutions for RPL

3 Related Work

This section presents the work done in the past related to the detection of anomalies in IoT networks.

Ioannou and Vassiliou (2019) proposed a c-SVM machine learning model to determine malicious and begin nodes. The proposed model achieved 100% detection of blackhole and sinkhole attacks and stated that the complexity of the c-SVM model depends on the location of the IDS in the network.

Anitha and Arockiam (2019) proposed an artificial neural network-based IDS system to detect DIS and version-number attacks in IoT. The proposed system was able to detect both RPL attacks very well; however, no algorithm was mentioned and no calculation was performed in terms of accuracy, precision, etc.

Han et al. (2022) focused on the difficulty of detecting anomalies in IoT networks with low data quality using machine learning. The authors concentrated on the system's overall performance, and resilience can be increased by combining several models or algorithms. The proposed algorithm can vary in different environments with diverse characteristics.

In this study (Janani and Ramamoorthy, 2022), the author proposed a threat analysis model that employs deep learning techniques to effectively identify and control routing attacks. The authors used the Mayfly optimization algorithm to optimize the features. The proposed methodology lacks computational efficiency and scalability.

In this study (Ali-Eldin 2022), the authors used trust in social IoT scenarios to identify trusted and untrusted users. User ratings were calculated based on different social aspects of the interaction of users in society. Furthermore, a machine learning algorithm was used to classify users. This method is used in social aspects of society; therefore, it requires heavy computation and updating of tables according to the parameters chosen for identification.

Saba et al. (2022) used the TON-IoT smart-city telemetry dataset to apply artificial intelligence techniques. The suggested methods were applied to seven TON-IoT datasets, including the garage door, thermostat, GPS tracker, and Modobus datasets. Compared to various voting classifier techniques such as Random Forest, ANN, and CNN, the proposed SMOTE voting classifier achieved 99.7% accuracy. The scalability and integration issues associated with implementing deep learning-based security frameworks in sizable smart-city IoT settings are not well covered by this study.

Authors in study (Sawafi et al. 2023) proposed Intrusion Detection system incorporates hybrid supervised and semi supervised machine learning algorithms used to identify RPL attacks. The proposed algorithm was based on Autoencoder and Artificial Neural Network. The proposed algorithm achieved better accuracy, but computation time is very high as the proposed algorithm used threshold calculation at two stages. However, system performs better in terms of detection accuracy but required complex calculations at hidden layers of the proposed algorithm.

In study (Shafi et al. 2023) machine learning and trust-based model is proposed by the authors. However, the authors considered the mobility parameters of a network in calculation of trust value of a node, but no proper algorithm is discussed. The model achieved better accuracy by considering 10-50 nodes.

In this study (Mahmood and Shafi 2023) authors focused on detecting zero-day attacks by using machine learning algorithm as multi-classifier. The proposed Intrusion detection system utilized Snort signature updating method for identification of anomaly in IoT systems. Although system achieved better accuracy as compared with other models, but no proper algorithm was designed for identification of malicious activities.

In this study (Dalal et al. 2023) authors enhance IoT security by utilizing multi class Support Vector Machine algorithm to classify the attack types. It employs an optimized CHAID decision tree to categorize the attack. Although it provides scalable solutions to handle the large volumes of IoT traffic with an accuracy 99.72%. But these types of models can be resource intensive and may struggle to adapt to new and emerging threats.

In this study (Albishari et al. 2022) authors used Advanced neural network models in deep learning-based early-stage detection (DL-ESD) for routing threats in Internet of Things (IoT) networks to detect and mitigate the attacks in their early phases. By analyzing network traffic patterns, DL-ESD aims to detect irregularities suggestive of routing attacks like blackhole, wormhole, or selective forwarding assaults, employing deep learning algorithms for this purpose. The primary goal is to minimize false positives while achieving high accuracy in identifying these types of attacks, emphasizing early detection to prevent or mitigate their adverse effects on IoT network security or performance. However, the implementation of DL-ESD may face challenges due to the significant computational resources required, making it potentially impractical for resource-constrained IoT devices or networks due to the associated computational overhead and energy consumption.

In this paper (Kim et al. 2024) authors proposed a framework that utilized the transfer learning process for detection of malicious behavior in the network. Detecting known and zero-day cyberattacks in IoT systems is an issue that these researchers seek to address by applying pre-trained model knowledge and optimizing it for IoT scenarios. High accuracy, low false prediction rates, and enhanced detection capabilities for a range of attack types are all displayed by the suggested solutions. The study also highlights the significance of customized models for 5G IoT scenarios with imbalanced and sparsely labeled information, demonstrating the potential of transfer learning to enhance IoT network cybersecurity.

The detailed literature survey of related studies is presented in Table 1 provided below. As the IoT landscape evolves, it is essential to continue to research and develop new technologies to remain ahead of cyber threats.

Table 1. Survey on related research studies.

Research Paper	Year	Methodology	Dataset	Results	Limitation
(Ioannou and	2019	Support Vector Machine	KDD	Accuracy=81%	Implemented on traditional dataset

Vassiliou 2019)					
(Anitha and Arockiam 2019)	2019	Artificial neural network and multilayer perceptron	NA	Not mentioned	Testing on traditional network
(Han et al. 2022)	2022	support vector machine (SVM), Logistic regression (LR), decision tree (DT), random forest (RF), naive Bayes (NB), multilayer perceptron (MLP)	KDDCup99 and Kitsune network attack	Not evaluated	Focuses on low quality data
(Janani and Ramamoorthy 2022)	2022	LSTM network and adaptive and Mayfly Optimization Algorithm (LAMOA)	Own dataset	accuracy:99.94% multiclass classification 99.92% accuracy for binary classifications,	Heavy computation is required due to optimization algorithm
(Ali-Eldin 2022)	2022	Social Trust and K nearest Neighbor	Brightkite dataSet	Accuracy:100%	Computation costs are very high. Trust calculation take more calculation time.
(Saba et al. 2022)	2022	SMOTE voting classifier, Random Forest, ANN, and CNN	TON-IoT datasets	Accuracy: 99.7%	Test size is very small, and number of trees increases complexity
(Sawafi et al. 2023)	2023	Autoencoder and Artificial Neural Network	IoTR-DS	Average Accuracy:98%	Computation cost is very high. Threshold calculation take more power consumption.
(Shafi et al. 2023)	2023	Support Vector Machine	NA	Accuracy: NIL	No proper algorithm was proposed; Machine learning parameters were not analysed.
(Mahmood and Shafi 2023)	2023	Support Vector Machine, Random Forest and K Nearest Neighbor.	CIC-IDS-2018	Accuracy:99.9%	Similarity index of the Snort Signatures is calculated but no proper algorithm was proposed.
(Dalal et al. 2023)	2023	CHAID and Support Vector Machine	Online IoT attack dataset	Accuracy:99.97%	More complex to implement, require significant computational power, having overfitting issue
(Al-bishari et al. 2022)	2023	Deep Neural Network	IRAD	Accuracy:98.85%	computational overhead and energy consumption.
(Kim et al. 2024)	2024	Transfer learning with CNN	Bot-IoT and IoT Intrusion	Accuracy:99.94%	Does not provide comprehensive comparison with other state-of-art techniques

As a result, artificial neural networks, and in particular deep learning algorithms, enhance IoT network security, ensuring smart devices and applications are protected from cyber-attacks.

4 Proposed Modelling

This section begins with a discussion of the neural networks (NN) topology. It then delves into the specifics of the loss function and concludes with a brief overview of the training procedure and algorithm that was used.

4.1Dataset

This section will outline the attributes (features) of the IRAD dataset as well as the modeling of the different attacks that result in traffic sample subsets (Yavuz et al. 2018). The attribute of dataset is presented in Table 2. When data packets reach the network layer, some routing attributes, DIO, DIS, Rank, and others are appended. Additionally, the root node will attach certain attributes, such receiving Time and total packets, that pertain to the data packet. The literature claims that these characteristics are helpful, and that the IDS system uses them to look for unusual activity. Normally, the values of nodes may change when they are joined to a tree, have their parent changed, or rank changed. It is expected that the network will be affected when malicious nodes initiate an attack. The basis of our detection system is the idea of trust. The degree of confidence a single thing has over another to do a task successfully and without compromising security is known as trust.

The three aspects that are most important taken into consideration are contextual information, service quality, and peer-to-peer communication quality. The security requirements to handle attacks in the IoT mobile environment are addressed by these dimensions. The dynamic and adaptable approaches that are employed in trust calculation and mechanism provision were used. Additionally, these methods improve network performance. The necessary parameters must be considered to carry out the analysis. The transaction history and weight assigned to each parameter are used to determine how well a device performs overall in terms of services supplied. Generally, the packet delivery ratio of the network, availability, throughput, and proportion of successful interactions as factors for assessing the quality of the service (Ali-Eldin 2022) (Alghofaili and Rassam 2022).

Table 2. Attributes of IRAD dataset (Yavuz et al. 2018).

Name/Abbreviation	Description
TIME	Simulation time
SOURCE	Source Node IP
DESTINATION	Destination Node IP
LENGTH	Packet Length
INFO	Packet Information
TR	Transmission Rate(per 1000_ms)
RR	Reception Rate(per 1000 ms)
TAT	Transmission Average Time
RAT	Reception Average Time
TPC	Transmitted Packet Count(per second)
RPC	Received Packet Count (per second)
TTT	Total Transmission Time
TRT	Total Reception Time
DAO	DAO Packet Count
DIS	DIS Packet Count
DIO	DIO Packet Count
CATEGORY	Attack Type or Normal
LABEL	Normal/Malicious Label

Our approach to this dimension includes both direct information and observations, including information history as well as direct information from recent years. The sum value of trust between entity A and entity B is determined by combining the calculated trust across many dimensions using equation 1.

$$T^{A,B} = \sum_{i=1}^{n} w1(\mathrm{PDR}) + w2(\mathrm{Average\ Delay}) + w3(\mathrm{Throughput}) \quad (1)$$

Where w1+w2+w3=1

T represents the total trust from node A to Node B and w1, w2 and w3 are the weights that influence the trust levels during the transactions in the network.

4.2Data Preprocessing

The first phase of the framework is presented in this section. Pre-processing of the data is done before training the DL models. Network traffic must be properly pre-processed for DL models to predict results without bias and to prevent overfitting issues. Data processing and feature selection are the two phases of pre-processing.

Every feature is converted to a floating-point value. This implies that all IP addresses are treated as distinct integers in the IRAD dataset, thus considering all network sizes. Because there are fewer features in the dataset, feature selection is not necessary. In both cases, traditional normalization of the dataset is then carried out to avoid DL model overfitting and potentially skewed outcomes.

4.3Avoid Overfitting

To counteract the overfitting tendency in DL, our framework incorporates specific strategies to ensure the authenticity of results. These methods enable the models to simulate realistic scenarios and maintain equal probability for each type of attack encountered in IoT devices. Furthermore, we treat IP addresses as floating-point numbers to accommodate various network types. Additionally, we integrate dropout techniques in certain DL models to avert excessively high performance that may not be realistic.

This approach facilitates the exploration of optimal hyperparameter combinations to maximize model performance. Throughout this exploration, training and validation losses serve as key indicators in the fine-tuning process, thereby mitigating the risk of overfitting. Overfitting significantly impacts model performance by causing a model to learn the training data too well, including its noise and outliers. Because of this, some model perform abnormally well on training data, but poorly on unseen data due to their inability to generalize. As a result of overfitting, the model becomes overly sensitive to the training data, making it less accurate and reliable when predicting new, real-world data. Preventing overfitting is crucial for developing models that are robust and perform consistently across different datasets.

One approach to prevent overfitting is to omit IP addresses during dataset preprocessing. This ensures that the model isn’t exposed to the same attacker IPs in both training and validation sets, preventing it from memorizing specific numerical patterns associated with attacker IPs due to their absence. Understanding the behavior of IP attackers is essential for future preventative strategies that rely on tracking. A promising research direction could involve employing explainable AI to determine if there’s a tangible link between IP addresses and attack methodologies, particularly concerning DoS attacks.

4.4Attack Detection Framework

The neurons or nodes that make up a neural network are interconnected with one another. In machine learning, these networks process and learn from data and enable tasks such as pattern recognition and decision making.

Unlike pre-programmed systems, neural networks extract identifying features from data. Networks such as these can identify patterns, classify data, and make decisions based on that data. Input Layer receives data from external sources. Hidden Layers used to transform input data into valuable features (Mohammadazadeh et al. 2022). Output Layer provides the network’s response (e.g., predictions or classifications). Units (neurons) are interconnected with weighted connections.

Every connection has a weight that establishes how much of an impact one unit has on another. During training, these weights are adjusted to improve model performance. In the Internet of Things (IoT) ecosystem, artificial neural networks (ANNs) serve as crucial to enhancing security and identifying cyberattacks.

The security of each node is crucial for the overall trustworthiness of the IoT network. With secure and reliable nodes, the entire network benefits from a distributed attack detection system. This section outlines an innovative Contextual Based Attack Detection Architecture that positions attack detection processes closer to the node, utilizing distributed IoT nodes to scrutinize network traffic and pinpoint cyber threats. This approach enhances current models by facilitating faster local training and fine-tuning of parameters.

4.5Structure of Artificial Neural Network

Figure 3 depicts the ANN structure, which is mathematically represented as:

$$\gamma, \delta = \phi^{L}(t; \omega, b)$$

Where the function$\phi^L: h^+ \dashv h^4$ represents the neural network with L number of layers; t € h^+ is the input to the input layer and γ, δ € h are the outputs; ω € h^{n*n} and b € h^n are the artificial neural parameters.

An artificial neural network is a feed forward network where input is supplied to the first layer, input is supplied to the second layer, and so on. The fundamental equation of artificial neural network can be represented below:

$$x^i = \sigma(\omega^i . x^{i-1} + b^i), \qquad i \in \{0, \ldots\ldots\ldots L\}$$

Where i denotes the layer number, $\sigma^i: h^+ \dashv h^4$ the activation function that adds nonlinearity to the artificial neural network, ω^i and b^i are the weights and biases of the specific layers.

In our proposed model, a 5- layer neural network, i.e L=5 can be represented by:

$$x^1 = \sigma^1(\omega^1 x^0 + b^1)$$
$$x^2 = \sigma^2(\omega^2 x^1 + b^2)$$
$$x^3 = \sigma^3(\omega^3 x^2 + b^3)$$
$$x^4 = \sigma^4(\omega^4 x^3 + b^4)$$
$$x^5 = (\omega^5 x^4 + b^5)$$

Where $x^0 \varepsilon\, t$ and $x^5\ \varepsilon\ (\gamma, \delta)$,The output of the final layer is indication whether node is malicious or benign. The artificial neural network input layer, hidden layer and output layer is represented in Fig 3.

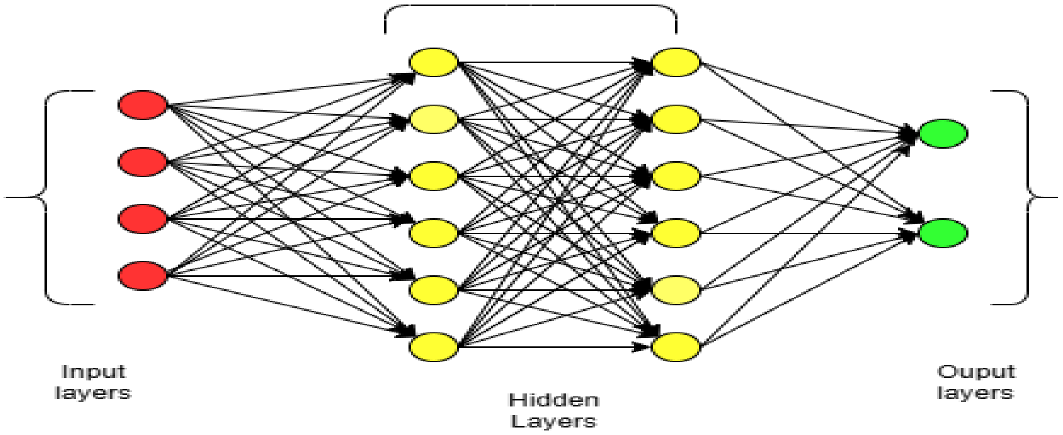


Fig. 3. Artificial Neural Network

The steps involved in pre-processing, model and gradient weight updates, and model validation are detailed in Algorithm 1, which outlines the distributed attack detection strategy.

Algorithm

Input: Balanced IRAD train dataset (Xtrain), learning rate(lr), training epochs(ep), batch size, test dataset (Xtest)

Output: Classification results

```
split the IRAD dataset into training dataset and validation dataset
drop the irrelevant features and insignificant features
select important features for ANN model
initialise weights and bias for j=1,,...., m, k=1,.......,n
initialise the ANN model with selected parameters
Repeat
for for input layer training epochs ep=1,2, ........., T do
    for for hidden layer neurons=1 to n do
        Train ANN network
        Calculate loss according to equation (2)
        Optimizing the ANN model by back propagation of loss function and also updating weights of ANN network
        Validation ANN model using validation dataset Xtest
    end
end
until Equation (1) gains maximum weights
```

16 Analyze test data to evaluate model performance on different metrices and predict attack types
17 Return model accuracy and loss

The architecture of the neural network is tailored based on the chosen deep learning ANN model and its intended function, which is detection, and on the specific dataset. The necessity to utilize distinct models for each dataset arises from the unique nature of the attacks encapsulated within them.

The ANN tailored for IoT attack detection within the IRAD dataset is structured with five hidden layers, containing 1250, 1000, 750, 500 and 250 neurons each, all utilizing ReLU activation functions. In the output layer a Softmax activation function is used. ReLU is chosen to prevent weight saturation, ensuring a continuous adjustment of weight values during training. For binary classification tasks like this one, mean absolute error is the preferred loss function, and Softmax is the only compatible activation function because it produces the necessary logarithmic outputs ranging from 0 to 1. Model is compiled using Nadam optimizers and mean absolute error losses over ten epochs. These parameters were empirically determined and fine-tuned using the Hyperband method.

Table 3. Hyperparameters of ANN model.

Parameters	Binary Classification
Number of Hidden layers	5
Number of neurons on hidden layers	7
Dropout	0.2
Activation Function in Hidden layers	ReLu
Activation Function in Output Layers	Softmax
Optimizer	Nadam
Loss Function	Mean absolute error
Learning rate	0.0001
No. of epochs	10

The current research paper's entire proposed modeling and architecture is presented in this section.

5 RESULTS

In our experimental setup, all deep learning models are developed using Keras with TensorFlow as the backend. Their performance is assessed using various metrics designed to validate and measure their effectiveness. These metrics include Accuracy (ACC), Loss, Precision, and Recall.

5.1Evaluation Metrices

These metrics can be derived from a confusion matrix—a tabular summary of the classification outcomes (refer to Table 5). In this matrix, True Positives (TP) and True Negatives (TN) represent the counts of attack and normal instances that are correctly identified, respectively. Conversely, False Positives (FP) and False Negatives (FN) represent the counts of normal and attack instances that are misclassified, respectively.

ACC, as defined is the ratio of accurately classified predictions to the total number of evaluated examples.

$$\textbf{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$$

Precision measures the proportion of accurately classified items to all predicted information.

$$\textbf{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

Recall is the proportion of all items that were class C to all items that were accurately classified as class C (attack or normal)

$$\textbf{Recall} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

Table 4 shows the confusion matrix of the predicted class normal and predicted class attack.

Table 4. Confusion Matrix.

		Normal Class (Predicted)	Attack Class (Predicted)
Actual	Normal	TN	FP
Class	Attack	FN	TP

The mean absolute error loss is the most widely used loss (see Eq. 2). Keep in mind that the y value indicates the actual output, while the Þ indicates the estimated output.

By computing the mean absolute error (MAE), which characterizes the change between the original and predictable values, the total change mean of the dataset is determined.

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} |y_i - \hat{y}_i| \qquad (2)$$

5.2Evaluation Results

We used several ratios based on the size and composition of the dataset, and the 0.2 ratio produced the best performance outcome. Additionally, the chosen ratio corresponds to the midpoint of our data, which is divided into 30% for the testing set and 70% for the training set. Using a biased evaluation function, assess the given model using the training dataset. Figure 4 illustrates that the rate of training epochs is suitable and can be deduced and in terms of accuracy during testing and training, the R-Trust model has done the best.

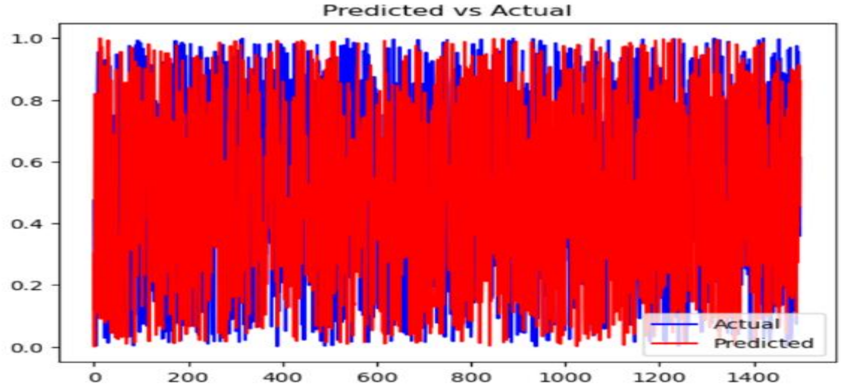


Fig. 4. shows the scatter plot of real and predicted values

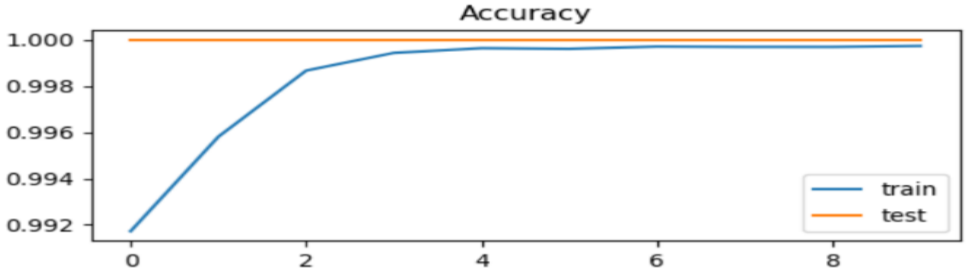


Fig. 5. shows the accuracy curve of the Proposed System

Among all the instances, accuracy is the percentage of instances correctly classified by the model. Essentially, the accuracy curve shows how well the model fits the training data, increasing its ability to make accurate predictions. Fig 5 shows that our model is better model and having high accuracy.

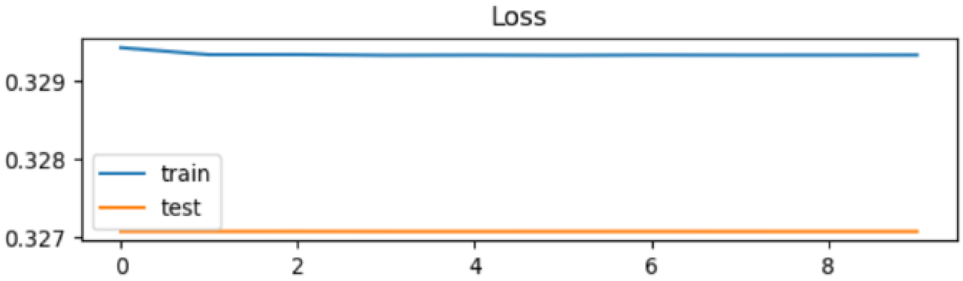


Fig. 6. shows loss curve which tells that during training and testing phase our model performs well and there is negligible loss of information

The maximum TPs, TNs, and fewest FN occurrences are effectively attained by the suggested detection technique. It is generally high for TN and it is the prediction ratio for TP's input values that determines classification. Meanwhile, for the malicious, classifier has a low-level FN and FP. Additionally, it shows that the classifier's performance and the predicted ratios meet expectations. Based on the DNN technique, the binary classification strategy is generated for the testing and training phases.

To gain a deeper understanding of the strength of the classifier, it is required to rely on classification reports because it is not possible to quantify the bias ratio among the classes in the classifier.

The performance measures for our model are compared in Table 5 with those of earlier studies that have utilized the same dataset and with recent studies that generated the IRAD dataset.

During training, our model included nine features with varying correlation levels for every attack. Although the suggested model evaluated the performance in comparison to a single classifier, the training results showed best results over IRAD dataset. On the other hand, ANN algorithms were used in our suggested classifier to assess performance accuracy. It is evident that our model is more effective with accuracy 99.80 in minimum number of epoch (10 epochs).

Table 5. Comparison of the related research and this research (✓: Topic is covered, ✗: Topic is not covered).

Related Research	Methodology	IoT Dataset	Contextual Information	Machine Learning Techniques	Accuracy	Loss
(Nayak et al. 2021)	GAN-C	IRAD	✓	Decision Tree	91	9.08
(Yavuz et al. 2018)	DNN	IRAD	✓	Deep neural Network	96.53	4.11
(Almusaylim et al. 2020)	SRPL-RP	✗	✓	✗	98.30	1.70
(Al-bishari et al. 2022)	DL-ESD	IRAD	✗	Deep neural Network	98.85	2.50
--	R-Trust	IRAD	✓	Artificial Neural Network	99.80	0.2

6 CONCLUSIONS

In conclusion, detecting and mitigating rank attacks in IoT devices is crucial to ensuring the security and reliability of interconnected systems. By understanding the methods for detecting such attacks, addressing common vulnerabilities, and recognizing the potential impacts of rank attacks, stakeholders can proactively safeguard IoT systems against malicious manipulation. As the IoT ecosystem continues to expand, vigilance and robust security measures are essential to protect against the evolving threat posed by rank attacks. This study includes contextual information for detection of routing attacks that is more important apart from other information of the network. A novel approach known as R-Trust has been implemented to identify routing attacks in network layers. The contextual features were extracted for the training model. Simultaneously, min–max scaling was used to standardize the data, removing the worst overfittings in training samples. The proposed model efficiently identified the normal and malicious nodes and attained better accuracy as compared with other models on same dataset. In future the model will be implemented with more routing attacks that dataset has covered and over the fog environment.

REFERENCES

1. Almusaylim, Z.A., Jhanjhi, N., Alhumam, A.: Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. Sensors. 20, 5997 (2020). https://doi.org/10.3390/s20215997.

2. Alsulaiman, L., Al-Ahmadi, S.: Performance Evaluation of Machine Learning Techniques for DoS Detection in Wireless Sensor Network. arXiv (Cornell University). (2021). https://doi.org/10.48550/arxiv.2104.01963.

3. Xu, H., Przystupa, K., Fang, C., Marciniak, A., Kochan, O., Beshley, M.: A Combination Strategy of Feature Selection Based on an Integrated Optimization Algorithm and Weighted K-Nearest Neighbor to Improve the Performance of Network Intrusion Detection. Electronics. 9, 1206 (2020). https://doi.org/10.3390/electronics9081206.

4. Yavuz, F.Y., Ünal, D., Gül, E.: Deep Learning for Detection of Routing Attacks in the Internet of Things. the International Journal of Computational Intelligence Systems/International Journal of Computational Intelligence Systems. 12, 39 (2018). https://doi.org/10.2991/ijcis.2018.25905181.

5. Al-Amiedy, T.A., Anbar, M., Belaton, B., Kabla, A.H.H., Hasbullah, I.H., Alashhab, Z.R.: A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. Sensors. 22, 3400 (2022). https://doi.org/10.3390/s22093400.

6. Darabkh, K.A., Al-Akhras, M., Zomot, J.N., Atiquzzaman, M.: RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. Journal of Network and Computer Applications. 207, 103476 (2022). https://doi.org/10.1016/j.jnca.2022.103476.

7. Musaddiq, A., Zikria, Y.B., Zulqarnain, Kim, S.W.: Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. EURASIP Journal on Wireless Communications and Networking. 2020, (2020). https://doi.org/10.1186/s13638-020-1645-4.

8. Alsukayti, I.S., Alreshoodi, M.: RPL-Based IoT Networks under Simple and Complex Routing Security Attacks: An Experimental Study. Applied Sciences. 13, 4878 (2023). https://doi.org/10.3390/app13084878.

9. Zhao, L.: A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header. (2021). https://doi.org/10.17487/rfc9035.

10. Onwuegbuzie, I.U., Razak, S.A., Isnin, I.F.: Control Messages Overhead Impact on Destination Oriented Directed Acyclic Graph—A Wireless Sensor Networks Objective Functions Performance Comparison. Journal of Computational and Theoretical Nanoscience. 17, 1227–1235 (2020). https://doi.org/10.1166/jctn.2020.8794.

11. Sawada, H., Kuriyama, H., Yusa, N., Mizuno, T., Mineno, H.: Mutually complementary communication protocol based on destination oriented directed acyclic graph. (2012). https://doi.org/10.1109/ccnc.2012.6181101.

12. Mohamed, K., Ali, S., Ali, S., Kassim, I.: Performance Evaluation of RPL and DODAG Formations for IoTs Applications. (2020). https://doi.org/10.23919/icitst51030.2020.9351340.

13. Sahay, R., Geethakumari, G., Modugu, K.: Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. (2018). https://doi.org/10.1109/wf-iot.2018.8355171.

14. Ali-Eldin, A.M.T.: A hybrid trust computing approach for IoT using social similarity and machine learning. PloS One. 17, e0265658 (2022). https://doi.org/10.1371/journal.pone.0265658.

15. Alghofaili, Y., Rassam, M.A.: A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. Sensors. 22, 634 (2022). https://doi.org/10.3390/s22020634.

16. Mohammadazadeh, A., Sabzalian, M.H., Castillo, O., Sakthivel, R., El-Sousy, F.F.M., Mobayen, S.: Neural Networks and Learning Algorithms in MATLAB. Springer Nature (2022).

17. Zahra, F., Jhanjhi, N.Z., Khan, N.A., Brohi, S.N., Masud, M., Aljahdali, S.: Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning. Applied Sciences. 12, 11598 (2022). https://doi.org/10.3390/app122211598.

18. Ioannou, C., Vassiliou, V.: Classifying Security Attacks in IoT Networks Using Supervised Learning. (2019). https://doi.org/10.1109/dcoss.2019.00118.

19. Anitha, A.A., Arockiam, L.: ANNIDS: Artificial Neural Network based Intrusion Detection System for Internet of Things. International Journal of Innovative Technology and Exploring Engineering. 8, 2583–2588 (2019). https://doi.org/10.35940/ijitee.k1875.0981119.

20. Han, S., Wu, Q., Yang, Y.: Machine learning for Internet of things anomaly detection under low-quality data. International Journal of Distributed Sensor Networks. 18, 155013292211337 (2022). https://doi.org/10.1177/15501329221133765.

21. Janani, K., Ramamoorthy, S.: Threat analysis model to control IoT network routing attacks through deep learning approach. Connection Science. 34, 2714–2754 (2022). https://doi.org/10.1080/09540091.2022.2149698.

22. Ali-Eldin, A.M.T.: A hybrid trust computing approach for IoT using social similarity and machine learning. PloS One. 17, e0265658 (2022). https://doi.org/10.1371/journal.pone.0265658.

23. Saba, T., Khan, A.R., Sadad, T., Hong, S.-P.: Securing the IoT System of Smart City against Cyber Threats Using Deep Learning. Discrete Dynamics in Nature and Society. 2022, 1–9 (2022). https://doi.org/10.1155/2022/1241122.

24. Sawafi, Y.A., Touzene, A., Hedjam, R.: Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. Journal of Sensor and Actuator Networks. 12, 21 (2023). https://doi.org/10.3390/jsan12020021.

25. Shafi, S., Mounika, S., Velliangiri, S.: Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET. Procedia Computer Science. 218, 2309–2318 (2023). https://doi.org/10.1016/j.procs.2023.01.206.

26. Mahmood, M., Shafi, Q.: A Smart IDS in IoT System to Detect Zero-Day Intrusions Using Automated Signature Update. Research Square (Research Square). (2023). https://doi.org/10.21203/rs.3.rs-3014508/v1.

27. Dalal, S., Lilhore, U.K., Faujdar, N., Simaiya, S., Ayadi, M., Almujally, N.A., Ksibi, A.: Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree. Journal of Cloud Computing. 12, (2023). https://doi.org/10.1186/s13677-023-00517-4.

28. Albishari, M., Li, M., Zhang, R., Almosharea, E.: Deep learning-based early stage detection (DL-ESD) for routing attacks in Internet of Things networks. the Journal of Supercomputing/Journal of Supercomputing. 79, 2626–2653 (2022). https://doi.org/10.1007/s11227-022-04753-4.

29. Kim, H., Park, S., Hong, H., Park, J., Kim, S.: A Transferable Deep Learning Framework for Improving the Accuracy of Internet of Things Intrusion Detection. Future Internet. 16, 80 (2024). https://doi.org/10.3390/fi16030080.

30. Nayak, S., Ahmed, N., Misra, S.: Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things. Ad Hoc Networks. 123, 102661 (2021). https://doi.org/10.1016/j.adhoc.2021.102661.