Al-Farabi Journal of Engineering Sciences Volume (4), Issue (2) December (2025)

ISSN: 2617-5517 (issn.org)
Al-Farabi Journal of Engineering Sciences
https://iasj.rdd.edu.iq/journals/journal/view/97
مجلة الفارابي للعلوم الهندسية تصدرها جامعة الفارابي

Hybrid Intrusion Detection Approach on the RPL Protocol for the Internet of Things

Ali Muwafaq Shaban
Department of Information Technology, College of Computer Science and Information Technology, University of Anbar, Ramadi 31001, Anbar, Iraq
Email: ali.m.shaban@uoanbar.edu.iq

Abstract
The Internet of Things (IoT) paradigm enables data transmission for multiple interconnected smart entities and requirements for fundamental and mission benefits across various sectors. IoT networks usually operate Routing Protocols for Low-Power and Lossy Networks (RPL). Nevertheless, RPL lacks protection components via configuration, presenting IoT-RPL as predisposed to low-overhead internal multiple types of attacks. Normal and attack traffic are usually similar, causing detection challenges for anomalies depending on signature-based intrusion detection systems (IDS). Additionally, a traditional explanation of the correctness of IDS techniques needs to be improved. This proposed a hybrid model of a one-dimensional convolutional neural network and decision tree (HODCNN-DT) approach. The experimental results show the proposed HODCNN-DT attack detection method's effectiveness. This approach enhances detection's precision, recall, and accuracy compared to other techniques.

Keywords: RPL, Internet of Things, Convolutional Neural Network, Intrusion Detection Systems, Machine learning.

1. Introduction

The main goal of the Internet of Things IoT is to connect every physical equipment connected to the Internet for easy access and usage in various application areas like healthcare, smart factories, and smart homes [1],[2]. These applications call for the capability to deploy huge sensor networks, devices that can both sense and actuate environmental processes, Radio Frequency Identification RFID and embedded systems in such a way that they can communicate with one another through the Internet by exchanging information without human mediation. Recently, the IoT has facilitated several industries like smart cities, agriculture, construction, and administrative automation. Routing and networking are essential parts of IoTs since they allow entities to communicate with one another. Many low-power wireless device sensors have been linked to the Internet and exist everywhere to provide more reasonable and universal services. The utilized sensors perform function-keeping and computing operations while exchanging data via lossy channels [3],[4].

Via permitting individuals and smart devices to intercommunicate anywhere, anytime, the large number of devices worldwide that are currently and will be in the future can intercommunicate through the Internet [5]. The sensors capture and share essential information from smart cities, smart home devices, and industrial units. Thus, the primary challenge in IoT is cyber security. Multiple IoT device sensors do not consider protection fundamentals similar to encrypting these data in transit appropriate to the limitations of the resources. IoT software defects are also uncovered regularly. Accordingly, investigators aim to develop alternative defense instruments appropriate for the IoT to protect the network protocol from attacks [6],[7].

The RPL is a protocol developed via the Internet Engineering Task Force (IETF) to manage the unavailability of a routing standard in IoT networks. It uses distance vector routing principles and Destination-Oriented DAG (DODAG) or Directed Acyclic Graph (DAG) for routing operations. It even has global and local rehabilitation agents responsible for fixing inconstancy issues, connection outages, and other protocol-related concerns. Regardless, the lightweight core of the RPL optional, protocol- and specification-dependent protection instruments expands the possibility of cyber-attacks [8]. Also, additional attacks on RPL have been occurring, like DoS, Selective Forwarding, Hello flooding, Sinkhole, Rank, Sybil, Neighbor, Version,

DODAG Information Solicitation (DIS), Local Repair, DAO Induction, Destination Advertisement Object (DAO) Inconsistency, and DAO Insider [9].

Multiple RPL attack detection techniques are presented to mitigate malicious activity and detect conduct. There are many detection agents that have been suggested, such as trust-based and acknowledgment-based. Between these agents, intrusion detection (ID) approaches have accepted high concentrations, allowing artificial intelligence (AI) to fight attacks, which has widely evolved into a significant research scope. Due to their detection performance, ID with deep learning (DL) and machine learning (ML) has been an up-and-coming resolution for RPL-IoT attack detection. These techniques can conduct massive heterogeneous IoT data and have the ability to detect brutal attacks with influential ID efficiency [10] , [11].

The problem statement can be identified as the most prominent barrier to routing in the IoT is security. IoT networks need more established and limited configuration principles, like the client-server paradigm. This deficiency makes using a comprehensive scope of conventional security resolutions in IoT networks impossible. Consequently, IoT is evolving into an advantageous platform for different Internet attacks as the number of Internet of Things devices increases. These attacks may accept multiple constitutions and target different resources on diverse IoT devices. For a particular IoT environment, continuous monitoring and analysis are required. ML and DL are practical techniques that can be involved in cyber security.

The key goal of the proposed hybrid RPL approach is to classify and detect various attacks and improve performance. The proposed develops the attack classification approach with improvements by extracting the best features by employing an ODCNN, then classifying multiclass by employing the DT technique to accomplish this goal.

Therefore, this article introduces HODCNN-DT to classify normal and four various RPL routing attacks (floating attack, blackhole attack, decreased rank attack, and DODAG version number attack). ODCNN was employed to extract the appropriate features from the dataset; then, we employed the DT technique to classify multiclass.

This study is structured in the following way: Section 1 gives the reviews of relevant literature. Research design, data collection, and analysis are presented in Section 3. Section 4, however, states and interprets the study's results. Lastly, Section 5 concludes the paper by summing up key insights, discussing implications and outlining future research avenues.

2. Related Works

This section examines various systems multiple authors have executed to identify attacks in RPL-based IoT networks. The related work can be explained below:

Sadasivam et al. [12] employed multiple types of ML techniques like multilayer perceptron (MLP), AdaBoost (AdB), decision trees (DT), logistic regression (LR), random forest (RF), Gaussian naive bayes (GNB), and K-nearest neighbors (KNN). All the technique's performance was evaluated utilizing performance metrics like Area Under the Curve (AUC), F1-score, recall, precision, and accuracy. The DT technique achieved the best performance with 92.6%, 0.946, 0.946, and 0.955 for accuracy, precision, recall, and F1-score, respectively, compared to all other techniques. The RF technique reached a higher AUC of 0.946 for the AUC metrics than all other techniques.

This study by Nayak et al. [13] proposed a DL-based routing attack detection method for industrial IoT using a generative adversarial network classifier (GAN-C). The study used a two-stage hybrid of GAN and SVM prototypes and utilized a detection and parallel learning representative to sustain DL on computationally restrained IoT sensors. The results compare distributed and centralized attack findings in the RPL network, showing a significant decrease in training time.

Sithik et al. [14] proposed a five-stage intelligent network security method, including registration of node information, multi-context-aware parent selection, congestion mitigation using MIAQ, the Deep Package Investigation and Attack Detection (LiteCNN-TL) algorithm, and an adaptive trickle timer. The results show improved performance in terms of packet loss ratio, delay, energy consumption, packet delivery rate, average control traffic overhead, and load balancing capability.

Kowsalyadevi et al. [10] proposed a DL-based multi-attack detection system designed to detect major routing attacks in IoT environments. The approach is structured into four phases: the first is data collection, the second is preprocessing, the third is feature selection, the fourth is data augmentation, and the fifth is attack classification. It utilizes min-max normalization, enhanced pelican optimization, data augmentation, and a hybrid DL model. Performance evaluations show IoBTSec-RPL accurately detects various RPL attacks in IoT environments, addressing class imbalances and enhancing overall security.

Bokka et al. [15] proposed a DL-based GRU network in this investigation to detect hazards in RPL-based IoT networks. The proposed approach dataset includes traffic traces for attack and normal scenarios like Blackhole, Sinkhole, DIO, Selective Forwarding, Sybil, and DIS flooding and suppression, with 21 attributes for 20 static nodes developed utilizing the NetSim Standard program. The GRU model was tested and trained with 20% and 80% of the dataset. The evaluation metrics employed in this investigation are f1-score, recall, accuracy, precision, and AUC. The findings prove the high efficiency of the proposed approach.

Khan et al. [16] proposed an approach consisting of prevention and detection algorithms established on random password generation (RPG) and comparison methods. The method then matches the passwords of communicating nodes, then approximates their constants and key IDs. Simultaneously, the prevention method specifies a delivery delay power in order to automate the participation of sensor nodes in communication. The proposed approach indicated better results than the allocated protection instruments regarding throughput, detection ratio, and intermediate delivery delay. The presented technique effectively mitigates side-channel and brute-force attacks in addition to Sybil attacks. The RPG-based detection and prevention approach can deliver powerful protection for RPL-based IoT networks.

Alazab et al. [17] proposed a hybrid intrusion detection system (HIDS) that combines DT and one-class SVM techniques to predict routing attacks. HIDS derives both SIDS and AIDS to identify prominent routing attacks in their depths. This dataset was also used to experiment on the presented HIDS, and it contains IoT network traffic and labels for other types of routing attacks. The results of the proposed HIDS approach in this investigation exceed those of the AIDS and SIDS methods, with heightened detection rates.

This study proposed a hybrid one-dimensional convolutional neural network-decision tree (HODCNN-DT) approach. model to improve attack detection accuracy in RPL-based IoT networks. It leverages DL strengths, incorporates advanced optimization techniques, and overcomes previous research challenges.

3. Proposed Hybrid RPL Attack Detection

In this section, we first describe the RPL dataset briefly. Then, the preprocessing operations that are performed on the dataset are explained. Then, we present the approaches of 1DCNN and DT classifiers. Lastly, we represent our proposed HODCNN-DT model for RPL attack detection as shown in Fig 1.

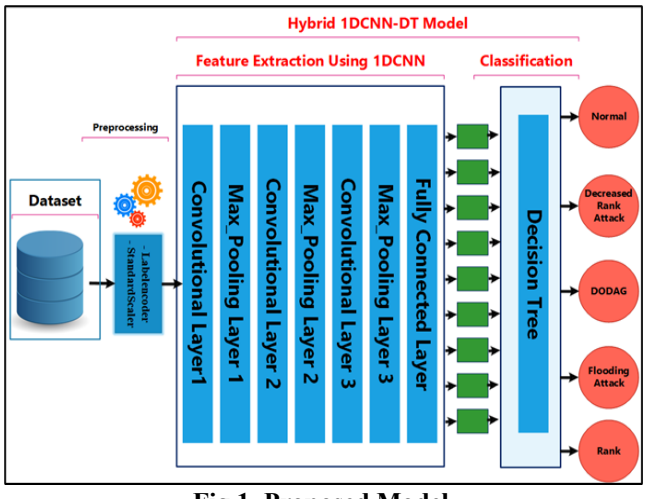


Fig 1. Proposed Model.

A - Dataset Description

The proposed approach utilized the available IEEE Data Port dataset (ROUT-4-2023: RPL-BASED ROUTING ATTACK DATASET FOR IOT) [18]. This dataset consists of a multiclass of normal and four many routing attacks (Decreased Rank Attack, DODAG Version Number Attack, Flooding Attack, and Blackhole Attack) established on the RPL protocol, and this dataset was acquired from Cooja (Contiki network simulator). The utilized dataset includes 1639976 instances; each instance has 16 features. Table I shows the feature description.

Table 1. Feature Description.

Feature	Description
TIME	The time of Simulation
SOURCE	The IP of Source Node
DESTINATION	The IP of Destination Node
LENGTH	The length Packet
TR	Transmission Rate(per 1000_ms)
RR	Reception Rate(per 1000 ms)
TAT	The Average Time Transmission
RAT	The Average Time of Reception
TPC	The Count Transmitted Packet (per second)
RPC	The Count Received Packet (per second)
TTT	The Time of Total Transmission
TRT	The Time of Total Reception
DAO	The Count of DAO Packet
DIS	The Count of DIS Packet
DIO	The Count DIO Packet
CATEGORY	Attack Type or Normal

B - Dataset Preprocessing

Data preprocessing is an important element in ML methods since the quality of the data and the relevant information that can be extracted from it have a direct impact on our models capacity to learn; hence, we must preprocess our dataset before delivering it to our model. Several preprocessing operations can be applied to data, depending on the nature of the data being used. Two preprocessing operations can be performed on the data used in the proposed approach. These are feature scaling and label encoding. Feature scaling is a data preprocessing process that changes the values of attributes in a dataset to a comparable scale. The objective is to confirm that all attributes contribute equally to the model and sidestep overwhelming attributes with larger values. When working with datasets including characteristics with varying ranges, feature scaling is important. In such instances, fluctuation in attribute values might result in biased model performance.. There are several standard methods for feature scaling. The proposed approach employed a standardization operation. This operation adjusts the feature values while maintaining their relative associations and distributions. It can be calculated from equation (1):

$$X_{Normalization} = \frac{x - mean(x)}{Standard\ deviation} \qquad (1)$$

The other preprocessing operation is label encoding. It is a method employed to transform categorical data into numerical form. This method assigns each unique label or class a unique numerical value. The

numerical values are allocated in an ordered way, starting from 0 or 1 and incrementing for each subsequent category. The proposed approach has five classes (blackhole attack, decreased rank attack, DODAG version number attack, flooding attack, and normal) assigned to (0, 1, 2, 3, and 4), respectively.

C - Proposed HODCNN-DT model

The proposed hybrid RPL attack detection approach based on HODCNN-DT is shown in Figure 1. The input of the approach is the entire RPL dataset features, and the output is a classification of five classes, which are either normal or four types of attacks. The approach includes two primary modules: the ODCNN and DT. The ODCNN module is employed to extract the best information on the characteristics of the RPL dataset, and the DT classifier module is utilized for RPL attack classification. First, train the ODCNN model, operate ODCNN to extract features associated to RPL attack, and also input the extracted features into the DT classifier for predection. Since the hyperplane learned by DT is the plane most distant from each category's selection point, DT's inference capability is more profitable than the original softmax. The two primary modules are explained in particular below:

ODCNN

CNN directs to a neural network that operates convolution functions in at least one layer of the network instead of standard matrix multiplication functions [19],[20]. Convolution is a particular linear function; each layer of the convolutional network usually contains at least three layers: the pooling layer, the convolutional layer, and the activation layer. Since the input of the utilized dataset is one-dimensional (OD), the ODCNN is employed to extract the appropriate characteristics [21]. The input of an ODCNN is 1D data; therefore, its convolution kernel, too, assumes an OD architecture. The output, too, coordinates to an OD feature vector. The fundamental design of ODCNN will be presented below: The Convolution Layer (CL) functions the convolution function on the OD input data and the OD convolution kernel and then extracts local characteristics via the activation layer. The CL functions as a convolution function on the OD input data and the OD convolution kernel, and then extracts local characteristics via the activation layer. The proposed ODCNN uses three CL with kernel_size = 2, strides = 1, and the activation function is ReLU. It is widely used because the Relu function congregates fast and can overpower the gradient dispersion. Thus, the Relu function is operated as the activation function. The hyperparameter settings of the ODCNN module are displayed in Table 2.

Table 2. ODCNN Model Parameter Hyperparameters.

Layer	Description	Parameter
Convolutional Layer 1	(None,16,64)	192
Max_Pooling Layer 1	(None,15,64)	0
Convolutional Layer 2	(None,15,128)	16512
Max_Pooling Layer 2	(None,14,128)	0
Convolutional Layer 3	(None,14,256)	65792
Max_Pooling Layer 3	(None,13,256)	0
Dropout	(None,16,64)	0
Flatten	(None,16,64)	0
Layer	Output Shape	Parameter
Convolutional Layer 1	(None,16,64)	192
Dense	(None,16,64)	426112

The pooling layer (PL) is usually involved after the CL. Down sampling prevents overfitting, decreases the network's spatial dimensions' parameters and features, and decreases the calculation complexity. The

features extracted via the CL are instructed into the PL to simplify the characteristics, maintain beneficial characteristics, decrease disproportionate characteristics, and make the extracted characteristics more reflective. In this analysis, the PL operates at maximum pooling. Finally, we use one layer of each dropout—a flattening and dense layer.

Decision Tree (DT)

The DT is a ML technique that uses a tree structure to develop rules for dataset classification [22]. It starts with the root node and moves towards a child node based on splitting criteria. The DT construction involves two phases: producing the tree and pruning it. Unlike most DT algorithms, the DT technique is top-down and starts with the root node, followed by intermediate nodes. The proposed approach uses DT for its advantages, including the ability to add new scenarios, select worst, average, and best values, and incorporate other decision strategies [23], [24].

D - Evaluation Metrix

Commonly utilized detection RPL attack evaluation indicators contain recall (R), precision (P), F1 score (F1), and accuracy (Acc). The F1 score and accuracy are used to estimate the model's overall performance [25]. Precision is utilized for prediction samples and correctly computes the number of samples predicted. The recall is founded on the original samples, and the number of samples is correctly predicted [26]. The formulas for precision, recall, accuracy, and F1 score are calculated in Equations 2, 3, 4, and 5, respectively, as follows [27],[28]:

$$p = \frac{TP}{TP+FP} \quad (2)$$

$$R = \frac{TP}{TP+FN} \quad (3)$$

$$Acc = \frac{TP+TN}{TP+FP+TN+TP} \ \ldots \quad (4)$$

$$F1 = \frac{P*R}{P+R} \ldots\ldots\ldots \quad (5)$$

The text outlines the classification of TP, FP, FN, and TN examples in a model. True positivity indicates a positive sample category, while false positivity indicates a negative category. False negative indicates a positive category but a negative model prediction. A true negative indicates a negative category, but a negative model prediction. The model's predictions are based on the true category of the sample.

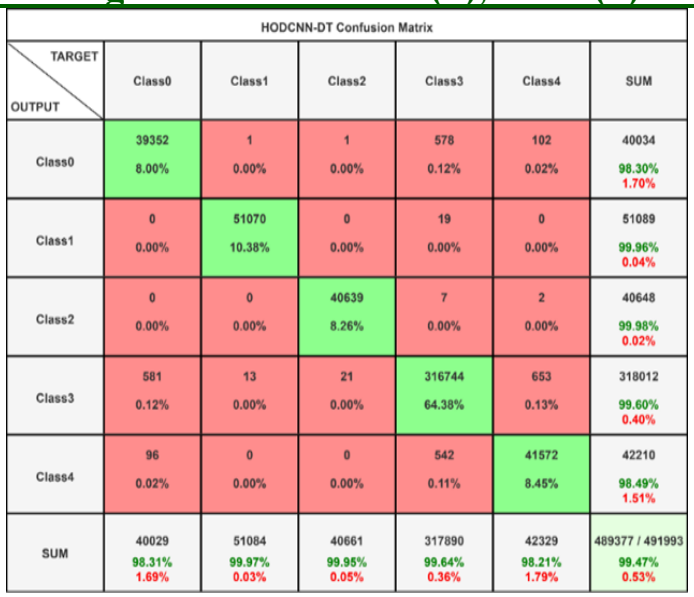
4. Result and Discussion

This study proposed a combination of a 1DCNN and a DT for the detection of RPL attacks. The model was designed to identify multiple classes, including normal traffic and four distinct routing attacks (decreased rank attack, DODAG type number attack, flooding attack, and blackhole attack). The proposed model shows good performance; it achieved a recall of 99.47%. The precision and accuracy of the model were also outstanding, both achieved at 99%, as summarized in Table 3 below.

Table 3. A Competition Results.

	Accuracy	Precision	Recall
Proposed model	99%	99%	99.47%

The confusion matrix shown in Fig. 2 contains a detailed breakdown of the model's performance across different classes. It clearly shows the model's ability to correctly classify the most common cases with very few misclassifications.



HODCNN-DT Confusion Matrix

TARGET / OUTPUT	Class0	Class1	Class2	Class3	Class4	SUM
Class0	39352 8.00%	1 0.00%	1 0.00%	578 0.12%	102 0.02%	40034 98.30% 1.70%
Class1	0 0.00%	51070 10.38%	0 0.00%	19 0.00%	0 0.00%	51089 99.96% 0.04%
Class2	0 0.00%	0 0.00%	40639 8.26%	7 0.00%	2 0.00%	40648 99.98% 0.02%
Class3	581 0.12%	13 0.00%	21 0.00%	316744 64.38%	653 0.13%	318012 99.60% 0.40%
Class4	96 0.02%	0 0.00%	0 0.00%	542 0.11%	41572 8.45%	42210 98.49% 1.51%
SUM	40029 98.31% 1.69%	51084 99.97% 0.03%	40661 99.95% 0.05%	317890 99.64% 0.36%	42329 98.21% 1.79%	489377 / 491993 99.47% 0.53%

Fig 2. Confusion matrix of proposed algorithm.

This proposed model achieved high accuracy, precision, and recall by combining two models (1DCNN and DT model), which highlights its effectiveness in detecting several RPL attacks. The model's ability to classify among normal traffic and different types of routing attacks with such high accuracy is a significant advancement in the field of IoT security.

5. Conclusions

This study proposed a hybrid of 1DCNN and DT to detect RPL attacks. This study aims to classify normal network behavior and these types of attacks. The proposed classifier has achieved the highest accuracy of 99%. This highlights the efficiency of the hybrid model in recognizing the difference between normal network behavior and RPL attacks. The findings of the proposed show the possibility of ML techniques for addressing security challenges in IoT networks, highlighting the need for further research and development to improve IoT security and the general implementation of IoT technologies in different domains. Future research should consider employing ensemble models for detecting RPL attacks in IoT networks. Ensemble models combine the predictions of multiple individual models, leveraging their diverse strengths and compensating for their weaknesses.

References

[1] R. D. Jalal and S. A. Aliesawi, "Enhancing TEEN protocol using the particle swarm optimization and BAT algorithms in underwater wireless sensor network," in *2023 15th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, 2023, pp. 504–510.

[2] N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, "Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon," *Baghdad Sci. J.*, vol. 21, no. 1, p. 234, 2024.

[3] T. A. Al-Amiedy *et al.*, "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet of Things*, vol. 22, p. 100741, 2023.

[4] M. Mahmood and B. Al-Khateeb, "Review of neural networks and particle swarm optimization contribution in intrusion detection," *Period. Eng. Nat. Sci.*, vol. 7, no. 3, pp. 1067–1073, 2019.

[5] S. Aliesawi, C. C. Tsimenidis, B. S. Sharif, and M. Johnston, "Performance comparison of IDMA receivers for underwater acoustic channels," in *2010 7th International Symposium on Wireless Communication Systems*, IEEE, 2010, pp. 596–600.

[6] M. Osman, J. He, F. M. M. Mokbal, N. Zhu, and S. Qureshi, "Ml-lgbm: A machine learning model based on light gradient boosting machine for the detection of version number attacks in rpl-based networks," *IEEE Access*, vol. 9, pp. 83654–83665, 2021.

[7] M. Mahmood, B. Al-Khateeb, and W. Alwash, "Review of neural networks contribution in network security," *Jour Adv Res. Dyn. Control Syst.*, vol. 10, no. 13, 2018.

[8] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and wormhole attack detection model for RPL-based internet of things using machine learning," *Sensors*, vol. 22, no. 18, p. 6765, 2022.

[9] M. Sheibani, B. Barekatain, and E. Arvan, "A lightweight distributed detection algorithm for DDAO Attack on RPL routing protocol in Internet of Things," *Pervasive Mob. Comput.*, vol. 80, p. 101525, 2022.

[10] K. Kowsalyadevi and N. V Balaji, "IoBTSec-RPL: A Novel RPL Attack Detecting Mechanism Using Hybrid

Deep Learning Over Battlefield IoT Environment," *Int. J. Comput. Networks Appl.*, pp. 637–650, 2023.
[11] S. A. Aliesawi, D. S. Alani, and A. M. Awad, "Secure image transmission over wireless network," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 2758–2764, 2018.
[12] R. Bokka and D. T. Sadasivam, "Machine Learning Techniques To Detect Routing Attacks in Rpl Based Internet of Things," *Int. J. Electr. Eng. Technol.(IJEET)*, vol. 12, pp. 346–356, 2021.
[13] S. Nayak, N. Ahmed, and S. Misra, "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things," *Ad Hoc Networks*, vol. 123, p. 102661, 2021.
[14] M. M. Sithik and B. M. Kumar, "Intelligent agent based virtual clustering and multi-context aware routing for congestion mitigation in secure RPL-IoT environment," *Ad Hoc Networks*, vol. 137, p. 102972, 2022.
[15] R. Bokka and T. Sadasivam, "Securing IoT Networks: RPL Attack Detection with Deep Learning GRU Networks," *Int. J. Recent Eng. Sci.*, vol. 10, no. 2, pp. 13–21, 2023.
[16] M. A. Khan, R. N. Bin Rais, and O. Khalid, "Collaborative Detection and Prevention of Sybil Attacks against RPL-Based Internet of Things.," *Comput. Mater. Contin.*, vol. 77, no. 1, 2023.
[17] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, and O. A. Mahdi, "Routing attacks detection in 6lowpan-based internet of things," *Electronics*, vol. 12, no. 6, p. 1320, 2023.
[18] M. H. Ö. Murat EMEÇ, "ROUT-4-2023: RPL Based Routing Attack Dataset for IoT," *IEEE Dataport*, 2024.
[19] M. A. Sameer, O. Bayat, and H. J. Mohammed, "Brain tumor segmentation and classification approach for MR images based on convolutional neural networks," in *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, IEEE, 2020, pp. 138–143.
[20] S. I. A. Al-Janabi, B. Al-Khateeb, M. Mahmood, and B. Garcia-Zapirain, "An enhanced convolutional neural network for covid-19 detection," *Intell. Autom. soft Comput.*, vol. 28, no. 2, pp. 293–303, 2021.
[21] A. A. Nafea, A.-M. Manar, K. M. A. Alheeti, M. S. I. Alsumaidaie, and M. M. AL-Ani, "A Hybrid Method of 1D-CNN and Machine Learning Algorithms for Breast Cancer Detection," *Baghdad Sci. J.*, vol. 21, no. 10, pp. 3333–3343, 2024.
[22] D. Loreti and G. Visani, "Parallel approaches for a decision tree-based explainability algorithm," *Futur. Gener. Comput. Syst.*, 2024.
[23] A. Suresh, R. Udendhran, and M. Balamurgan, "Hybridized neural network and decision tree based classifier for prognostic decision making in breast cancers," *Soft Comput.*, vol. 24, no. 11, pp. 7947–7953, 2020.
[24] M. S. I. Alsumaidaie, A. A. Nafea, A. A. Mukhlif, R. D. Jalal, and M. M. AL-Ani, "Intelligent System for Student Performance Prediction Using Machine Learning," *Baghdad Sci. J.*, vol. 21, no. 20, pp. 3877–91, 2024.
[25] O. J. Kadhim, A. A. Nafea, S. A. S. Aliesawi, and M. M. Al-Ani, "Ensemble Model for Prostate Cancer Detection Using MRI Images," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, 2023, pp. 492–497.
[26] X. Zhang, P. Han, L. Xu, F. Zhang, Y. Wang, and L. Gao, "Research on bearing fault diagnosis of wind turbine gearbox based on 1DCNN-PSO-SVM," *IEEE Access*, vol. 8, pp. 192248–192258, 2020.
[27] M. MAHMOOD and B. AL-KHATEEB, "TOWARDS AN AUTOMATIC GENERATION OF NEURAL NETWORKS.," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 23, 2017.
[28] A. Churcher *et al.*, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, 2021.