Enhancing internet of things security: evaluating machine learning classifiers for attack prediction

Areen Arabiat, Muneera Altayeb
Department of Communications and Computer Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received May 7, 2024
Revised Jun 29, 2024
Accepted Jul 5, 2024

Keywords:

Cyber attack
Internet of things
Intrusion detection system
Machine learning
Orange3

ABSTRACT

The internet of things (IoT) has contributed to improving the quality of service and operational efficiency in many areas, such as smart cities, but this technology has faced a major dilemma: the problem of cyber-attacks of various types. In this study, we relied on the use of machine learning (ML) and deep learning (DL) techniques to present a proposed model of an intrusion detection system (IDS) for detecting different types of IoT attacks that include ARP_poisoning, DOS_SYN_Hping, MQTT_Publish, NMAP_FIN_SCAN, NMAP_OS_DETECTION, and Thing_Speak. However, the proposed model is built using Orange3 data mining tools. The model consists of random forest (RF), artificial neural network (ANN), logistic regression (LR), and support vector machine (SVM) classifiers. On the other hand, the data set that is used was obtained from the Kaggle platform's real-time IoT infrastructure data set, called RT-IoT2022. The data set consists of a huge number of records, which are processed and then reduced to 7,481 records using linear discriminant analysis. In the next stage, the data set is fed to the Orange3 data mining tool, which is divided into 70% of the training dataset and 30% of the test dataset, in addition to using fold-cross validation to increase accuracy and avoid overfitting. Thus, the experimental results showed the superiority of RF with a classification accuracy of (99.9%), while the accuracy in ANN reached (99.8%), (97.8%) in LR, and finally, for SVM, the accuracy reached (92.9%).

Corresponding Author:

Areen Arabiat
Department of Communications and Computer Engineering, Faculty of Engineering, Al-Ahliyya Amman University
Al-Salt, Amman, Jordan
Email: a.arabiat@ammanu.edu.jo

1. INTRODUCTION

Recently, the internet of things (IoT) is a system that combines different technologies and devices, doing away with the necessity for human interaction. As a result, smart cities that promote comfortable, productive, and sustainable living have been created. Through the integration of information and communications technology (ICT) in government, transportation, housing, business, sustainable living, social learning, community participation, and other areas, smart cities seek to improve the quality of life for their citizens [1]. Protecting against multiple cyberattacks and maintaining cybersecurity have become urgent concerns. The primary cause of this is the exponential expansion of computer networks and the multitude of pertinent applications that people and organizations utilize for personal or business purposes, particularly with the adoption of the IoT [2]. IoT has attracted interest from a wide range of industries, including healthcare, logistics monitoring, smart cities, and the automotive industry. But as a paradigm, it is sensitive to several serious attack risks [3]. A global network of smart devices that are connected is also defined as IoT. It affects human activities and becomes a target for criminal behavior. The ecosystems of IoT depend substantially on cybersecurity, yet conventional approaches are inadequate because of complex design and new threats [4]. Cyber-physical systems (CPSs) are computerized systems that are employed in many industries, including manufacturing, energy, healthcare, and the military. IoT is critical to the development of sustainable infrastructure because related infrastructures depend on smart devices' capacity for internet-based communication [5]. IoT environment monitoring, network data packet analysis, and real-time reaction generation are all made possible by the intrusion detection system (IDS). Nevertheless, they have to function in extreme environments, such as those with limited energy, low process capacity, quick reaction times, and high quantities of data processing. Improving IoT-embedded IDSs necessitates an ongoing awareness of vulnerabilities in security. The fast progress of the internet and communication technologies presents difficulties for network security in terms of precisely identifying breaches and averting assaults. Potential solutions being implemented for IDS systems are machine learning (ML) and deep learning (DL) [6], [7].

Peer-to-peer networks and blockchain users are the targets of increasing numbers of attacks using the denial of service (DoS) attack vector. Blockchain improves security, but it is still accessible to new attack threats because of its decentralized architecture, encrypted distributed storage, and privacy features. The fact that blockchain is mostly utilized for financial applications means that if a DoS effort is successful, the damage will probably be enormous. Research to date does not provide a comprehensive description of the state-of-the-art for potential DoS and related mitigation approaches [8]. Distributed denial of service (DDoS) attacks damage cloud services and cause problems for authorized users by overloading network infrastructure with requests. Fraudulent data collection, hacking, political disagreements, vandalism, and corporate competition are among the primary factors. Examples include modifying devices to function as externally controlled bots, which can cause a partial or whole denial of service. Different consequences affect traditional networks, including lost revenue, interruptions of service, damage to brand equity, and attack mitigation expenses [9]. Artificial intelligence (AI) has transformed several industries by making it possible to create functional systems for jobs that were previously thought to be imaginative. AI-enabled security systems provide instantaneous network data analysis, alert triggering, and person identification capabilities. Researchers are now extending sophisticated systems with security layers since these complex structures are vulnerable to attacks. Data scientists are currently dealing with new ML challenges in data science, such as clustering, classification, prediction, and regression, due to the rapid growth and huge volume of data generated by the IoT [10]. ML systems fulfill IoT security requirements by being scalable, strong, and adaptive. On the other hand, present IoT topologies, security risks, and network weaknesses create challenges for conventional methods.

Bagaa *et al.* [11] presented a study describing an ML-based security architecture for the IoT. By leveraging software defined networking (SDN) and network function virtualization (NFV) to reduce risks, the framework integrates monitoring and response agents, ML models, and anomaly detection for IoT devices. Experiments showed the effectiveness of the proposed system, which uses data mining to identify attacks with high performance and low cost. In a realistic smart building scenario, the anomaly detection system obtained a detection accuracy of 99.71%. Hussain *et al.* [12] presented a two-step ML strategy to prevent and detect botnet attacks on IoT. The first phase trains a DL model, ResNet-18, to detect scanning activity during an attack, while the second phase trains another ResNet-18 model to identify distributed denial-of-service (DDoS) attacks. The proposed method achieves 98.89% accuracy, 99.01% precision, 98.74% recall, and 98.87% F1-score. Rahman *et al.* [13] presented a model to predict several cyber-attacks (DDoS, Port Scan, Bot, Brute Force, SQL Injection (SQLi), and Heartbleed), where the proposed system first extracts patterns related to cyber-attacks from historical data using the J48 decision tree (DT) algorithm and then builds a prediction model to predict cyber-attacks. Futurism is the system was trained on a dataset provided by the Canadian Cybersecurity Institute. The overall accuracy of the proposed prediction model for detecting cyberattacks was about 99%. Ahuja *et al.* [14] used SDN to provide an ML approach to classify benign network traffic from ARP-poison and ARP-flooding attacks. Mininet was used to create a Python application that collects and records attack features. With an accuracy of 99.73%, the hybrid convolutional neural network-long short-term memory (CNN-LSTM) model performs better than other ML models.

On the other side, Khan *et al.* [15] presented a study based on a deep neural network (DNN) model to detect intrusions in message queuing telemetry transfer (MQTT)-based protocols. The proposed model was then compared with traditional machine-learning algorithms. For single flow, dual flow, and bundle flow, the model accuracy was 99.92%, 99.75%, and 94.94%, respectively. However, the accuracy decreased to 97.08%, 98.12%, and 90.79% using multi-label classification. When comparing the DNN model to long short-term memory (LSTM) and gated recurrent units (GRUs), it had the highest accuracy at 97.13%. Binu *et al.* [16] presented a unique SDN-based early detection and mitigation approach for unusual IoT activity. Healthcare, agriculture, and other smart home networks can all benefit from it. The concept ensures double-layer protection by identifying threats in SDN controllers and gateway devices. Thus, a 98.5% accuracy rate was demonstrated using real-time DoS attacks on an IoT network based on the Thing Speak cloud. Dutt *et al.* [17] presented a model for computer network intrusion detection based on statistical modeling anomaly detection (SMAD), which imitates the body's immune system. Anomalies in questionable network packets were identified by the second layer, adaptive immune-based anomaly detection (AIAD). A 96.04% true positive rate for SMAD and a 97% true positive rate for AIAD were demonstrated by experiments conducted on standard datasets and real-time network traffic.

Pooja *et al.* [18] used the complicated datasets KDDCUP-99 and UNSW-NB15 to create an automated approach for detecting network intrusions. The model, created utilizing the LSTM approach, was performed with 99% accuracy. The work focuses on the application of DL methods and a bi-directional LSTM-based identification model. The model worked well with several activation functions, reaching an average accuracy of 99.5%. The results were compared with cutting-edge approaches. Ullah *et al.* [19] introduced a hybrid DL model consisting of LSTM and GRU for cyberattack detection on the internet of vehicles. The combined DDoS dataset and the car-hacking dataset were used to examine the performance of the suggested model. The testing findings showed that the suggested method successfully detects attacks with an accuracy of 99.5% for DDoS attacks and 99.9% for automobile hacks. Mihoub *et al.* [20] investigated the use of ML to identify DoS/DDoS attacks on IoT devices. It offers a novel architecture that consists of two parts: DoS/DDoS detection and mitigation. The detection component identifies the attack type and packet type using a multi-class classifier with a “Looking back” concept, allowing mitigating techniques to be applied. The looking-back-enabled random forest (RF) classifier achieved 99.81% accuracy on the Bot-IoT dataset, according to the assessment findings. Musleh *et al.* [21] evaluated several feature extraction models and methods to investigate ML as an intelligent identifier on the IoT. Image filters, RF, K-nearest neighbors, support vector machine (SVM), stacked models, and transfer learning models such as VGG-16 were evaluated. and DenseNet. According to the study, stacking with VGG-16 produced the best accuracy of 98.3%. Ivanova *et al.* [22] presented two types of classifiers for DDoS attacks based on SVM-binary and multi-class, where ten common attacks were studied and the detection rate, classification accuracy, and other parameters were measured. SVM was found to be the most accurate, achieving a classification accuracy of up to 99.9% for some attacks.

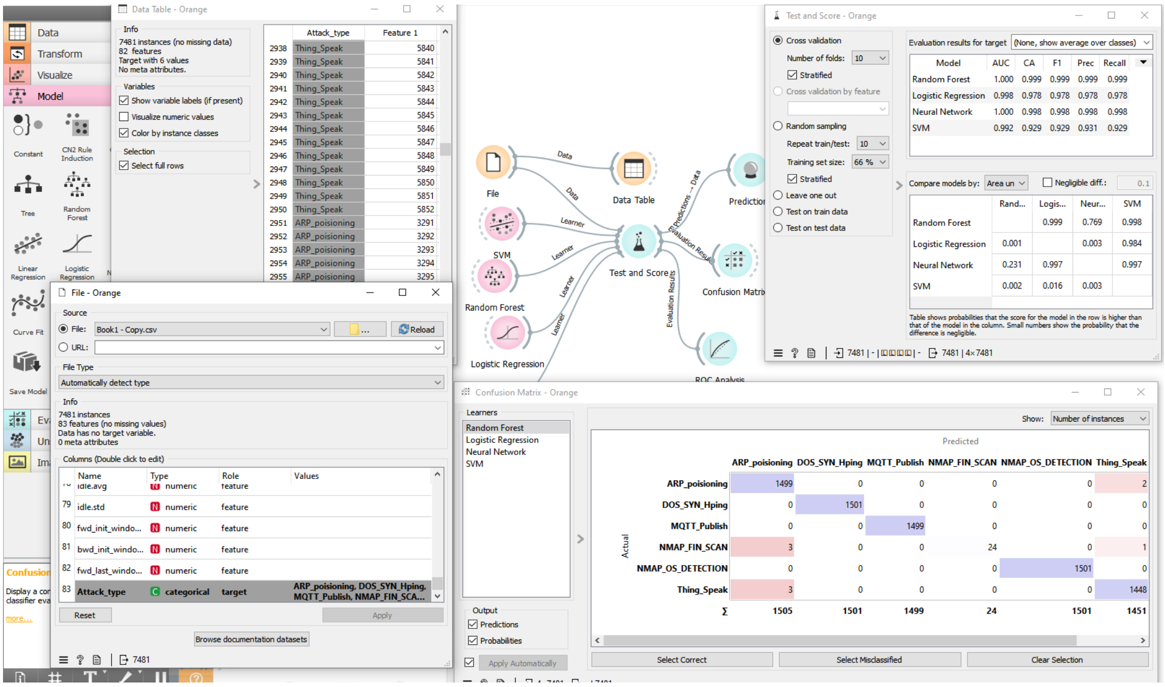
The novelty in this work is deployed by developing a predictive model using both ML and DL techniques. The model includes RF, SVM, logistic regression (LR), and artificial neural network (ANN) to identify different types of IoT cyber-attacks. However, the selected classifiers were chosen because they demonstrate a careful application of modeling strategies, which raises the validity and interpretability of the findings, and they demonstrate efficacy in detecting IoT attacks using a registered dataset from Kaggle. The novel aspect is summarized by using all the mentioned classifiers together and using a huge data set in addition to using the Orange3 data mining tool.

2. METHOD

The detection and evaluation of cyberattacks in IoT applications is based on ML and DL learning in a large number of published papers. To identify various IoT threats, a novel ML and DL model was utilized. First, a registered dataset, including 7,481 records of various attack types and 83 features, was obtained from Kaggle. The data set had preprocessing, which included removing enormous, irrelevant, and missing data to make it appropriate for feeding into the Orange3 tool in CSV format. After that, a classification model was constructed using the four fundamental algorithms for attack detection: RF, ANN, LR, and SVM features, which were fed to the Orange3 data mining package to find and visualize the result of the model classification as shown in Figure 1 which depicts the model of IDS using Orange3. The potential of Orange3, an open-source data mining and machine learning framework, in practical internet of things systems is investigated in this study. Predictive models for the automation of smart homes for example and anomaly detection for industrial asset monitoring are recommended. Nevertheless, there are still difficulties in handling noisy sensor data, controlling systems, and integrating models with current systems. The study concludes that Orange3 can offer an adaptable framework for putting these models through testing, deployment, and validation for use in practical settings. So far, it can be one of the limitations of this study.

2.1. Proposed model

Five main stages are often involved in developing a model using ML and DL techniques, as shown in Figure 2. Data preparation, feature selection, data reduction, testing and training, and result evaluation. The dataset is preprocessed for each of the suggested solutions to convert it into a format that the algorithm can use. This stage also involves cleaning the dataset, which typically involves deleting items that include duplicates or missing data. The training dataset and the testing dataset are then created by randomly dividing the preprocessed data. In this research, the training dataset makes up around 70% of the initial dataset, with the remaining 30% being the testing dataset, to enable the model to reach a reasonable result with 7,481 records and 83 features. Consequently, 10-fold cross-validation was also applied to improve the results and avoid overfitting. However, the size of the dataset and the complexity of the suggested model determine how long the algorithm takes to learn. So far, the dataset's feature selection, data cleaning, linear discriminant analysis, and accurate data preprocessing have enhanced classification effectiveness, data complexity, accuracy, and model performance in datasets. According to the training phase, the ML algorithm is subsequently learned with the training dataset. After the stage of training, the model is tested and evaluated according to its predictions. Using IDS models, it will be predicted if the network has a cyber security attack. In the final stage, the dataset is evaluated based on f-measure, accuracy, sensitivity, and precision once the trained model has been constructed. Using the confusion matrix, the effectiveness of the classifiers trained in the suggested model will be assessed. To determine which ML model has the best performance metrics, the acquired results will also be compared. Figure 2 depicts the flow diagram of the proposed IDS.



Data Table - Orange

Info
7481 instances (no missing data)
82 features
Target with 6 values
No meta attributes.

Variables
☑ Show variable labels (if present)
☐ Visualize numeric values
☑ Color by instance classes

Selection
☑ Select full rows

	Attack_type	Feature 1
2938	Thing_Speak	5840
2939	Thing_Speak	5841
2940	Thing_Speak	5842
2941	Thing_Speak	5843
2942	Thing_Speak	5844
2943	Thing_Speak	5845
2944	Thing_Speak	5846
2945	Thing_Speak	5847
2946	Thing_Speak	5848
2947	Thing_Speak	5849
2948	Thing_Speak	5850
2949	Thing_Speak	5851
2950	Thing_Speak	5852
2951	ARP_poisioning	3291
2952	ARP_poisioning	3292
2953	ARP_poisioning	3293
2954	ARP_poisioning	3294
2955	ARP_poisioning	3295

File - Orange

Source
● File: Book1 - Copy.csv
○ URL:

File Type
Automatically detect type

Info
7481 instances
83 features (no missing values)
Data has no target variable.
0 meta attributes

Columns (Double click to edit)

	Name	Type	Role	Values
78	idle.avg	N numeric	feature	
79	idle.std	N numeric	feature	
80	fwd_init_windo...	N numeric	feature	
81	bwd_init_windo...	N numeric	feature	
82	fwd_last_windo...	N numeric	feature	
83	Attack_type	C categorical	target	ARP_poisioning, DOS_SYN_Hping, MQTT_Publish, NMAP_FIN_SCA...

Reset Apply
Browse documentation datasets
7481

Test and Score - Orange

● Cross validation
Number of folds: 10
☑ Stratified
○ Cross validation by feature
○ Random sampling
Repeat train/test: 10
Training set size: 66 %
☑ Stratified
○ Leave one out
○ Test on train data
○ Test on test data

Evaluation results for target (None, show average over classes)

Model	AUC	CA	F1	Prec	Recall
Random Forest	1.000	0.999	0.999	0.999	0.999
Logistic Regression	0.998	0.978	0.978	0.978	0.978
Neural Network	1.000	0.998	0.998	0.998	0.998
SVM	0.992	0.929	0.929	0.931	0.929

Compare models by: Area un ☐ Negligible diff.: 0.1

	Rand...	Logis...	Neur...	SVM
Random Forest		0.999	0.769	0.998
Logistic Regression	0.001		0.003	0.984
Neural Network	0.231	0.997		0.997
SVM	0.002	0.016	0.003	

Table shows probabilities that the score for the model in the row is higher than that of the model in the column. Small numbers show the probability that the difference is negligible.

7481 | - | - 7481 | 4×7481

Confusion Matrix - Orange

Learners
Random Forest
Logistic Regression
Neural Network
SVM

Output
☑ Predictions
☑ Probabilities
☑ Apply Automatically

Show: Number of instances

Actual \ Predicted	ARP_poisioning	DOS_SYN_Hping	MQTT_Publish	NMAP_FIN_SCAN	NMAP_OS_DETECTION	Thing_Speak
ARP_poisioning	1499	0	0	0	0	2
DOS_SYN_Hping	0	1501	0	0	0	0
MQTT_Publish	0	0	1499	0	0	0
NMAP_FIN_SCAN	3	0	0	24	0	1
NMAP_OS_DETECTION	0	0	0	0	1501	0
Thing_Speak	3	0	0	0	0	1448
Σ	1505	1501	1499	24	1501	1451

Select Correct Select Misclassified Clear Selection

Figure 1. Intrusion detection system model using Orange

2.2. Dataset

One unique dataset from real-time IoT infrastructure, RT-IoT2022, was obtained from Kaggle and offers a thorough understanding of network behavior in both hostile and normal settings. It contains a huge number of simulated records of attacks from several IoT devices. The security environment is improved by using the dataset to create strong security solutions for real-time IoT networks and to improve the capabilities of IDS. One of the most important ML pre-processing steps is feature selection. It improves the effectiveness of the classification process and decreases the complexity of the data. Several feature selection techniques for IDSs were proposed by academics. These techniques are suggested for categorizing significant characteristics according to several standards [23].

2.3. Machine learning classification

Machine learning (ML) is a subfield of AI that enables computers to learn by analyzing data automatically, without explicit programming [24]. Three main areas comprise ML: reinforcement learning (RL), unsupervised learning, and supervised learning. RL entails executing tasks iteratively and modifying behavior in response to feedback; supervised learning deals with issues with labeled instances; and unsupervised learning finds patterns in unlabeled data [25]. ML models that have been trained to categorize input data into discrete classes, each with unique advantages and disadvantages, are called classifiers [26].

2.3.1. Random forest

Random forest is a combination of DT models that aims to achieve precision and avoid overfitting while avoiding unbalanced datasets. It uses the DT idea to select a random sample of data and evaluate each

DT's unique error rate to identify the best combination of variables for classification. The formula for majority voting-based class label prediction is used as shown in (1) [27], [28].

$$I(y) = argmaxc\ (\sum_{n}^{N}\ T_{hn}(y)\ ) = 0 \tag{1}$$

In this case, I depict the indicator function and h_n is the RF's n^{th} tree.

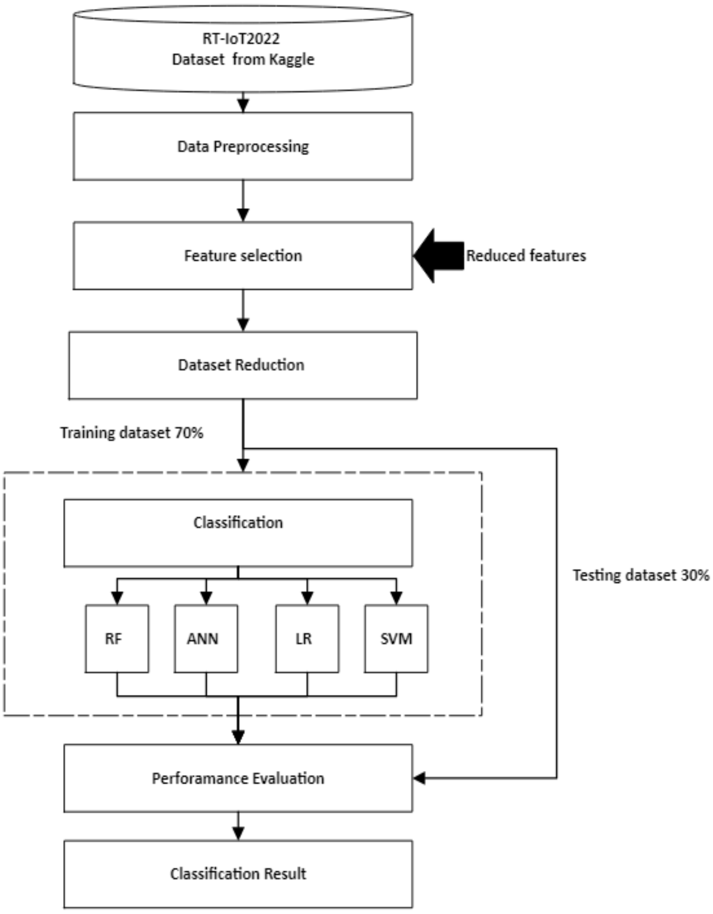


Figure 2. Flow diagram of the proposed intrusion detection system method

2.3.2. Logistic regression

Is a statistical technique used to examine datasets and provide binary results based on autonomous variables that are binary. The best uses for this approach are in the prediction of binary and categorical outputs. It predicts both of the independent variable categories and controls the impact of other independent variables. The maximum likelihood technique is used to create the best-fitting function to maximize the possibility that the data will be classified into the correct division [29]. The LR model is described in (2):

$$\frac{Prob(Yi=1)}{Prob(Yi=0)} = \frac{Pi}{1-Pi} = e(\ \beta 0 +\ \beta 1\ X1 + \cdots \ldots +\ \beta k\ Xki) \tag{2}$$

where Pi is the probability that Y will take a value of 1, e is the exponential constant, and $(1 - Pi)$ is the chance that Y will take a value of 0 [30].

2.3.3. Artificial neural network

Is a machine-learning technique that replicates human brain neurons using multi-layered ANN and large amounts of data. It has proven effective in applications like speech recognition, object identification, and illness diagnosis. Neural networks like recurrent neural network (RNN), ANN, and CNN are preferred for feature engineering and decision-bounding in DL challenges, autonomous vehicles, and unmanned aerial vehicles [31], However, ANN consists of up to three layers: an input layer, an output layer, and one or more hidden layers. It has many fundamental unit neurons that conduct layer-by-layer conduction between neurons to transmit signals, as shown in Figure 3 [32]. Every neuron in the input layer (designated by $X_1, \ldots, X_k$) in the input layer. In order to the concealed layer, the input variables expanded as shown in (3).

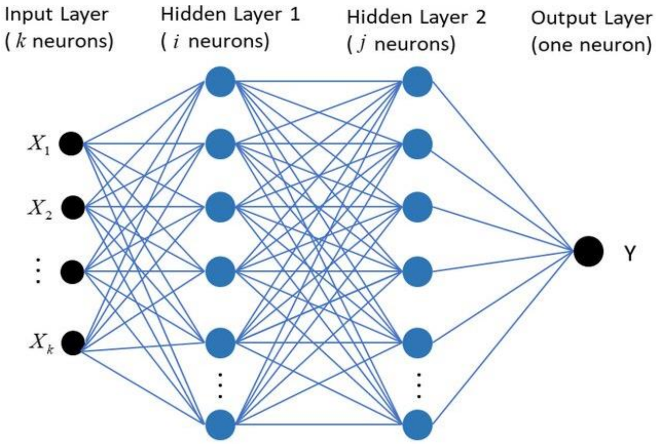


Figure 3. Architecture of neural network [33]

$$Si = \sum_{k=1}^{N} \quad W_{ki} \quad X_k + \quad b_i \tag{3}$$

where W_i is the weight value of the link between neurons k from the input layer and neurons i from the first hidden layer, Si is the ith output in the first hidden layer, and bi is the value of the bias value associated with neuron i. The preceding layer's output was assigned as input and propagated to the following layer for the second hidden layer [34].

2.3.4. Support vector machine

To divide linearly separable data samples into two classes, the hyperplane with the largest margin is sought after. SVM maps the data into a high-dimensional feature space and does classification if there is nonlinearly separable data. Equations for positive and negative samples define the canonical hyperplane, which has support vectors on it [35], [36]. Figure 4 depicts the structure of SVM.

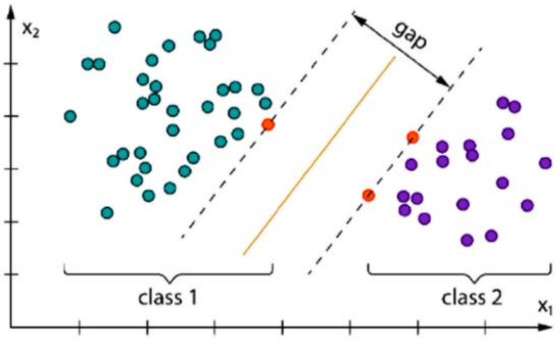


Figure 4. Structure of SVM [37]

2.4. Orange3 data mining tool

Is an open-source data mining toolkit used for exploratory data analysis and visualization. It is built on Python, acts as an experiment selection platform, and is useful when innovation, reliability, or quality are required. Orange may be used on the command line or in any Python context to offer a well-structured overview of various features [38], [39].

3. PERFORMANCE EVALUATION

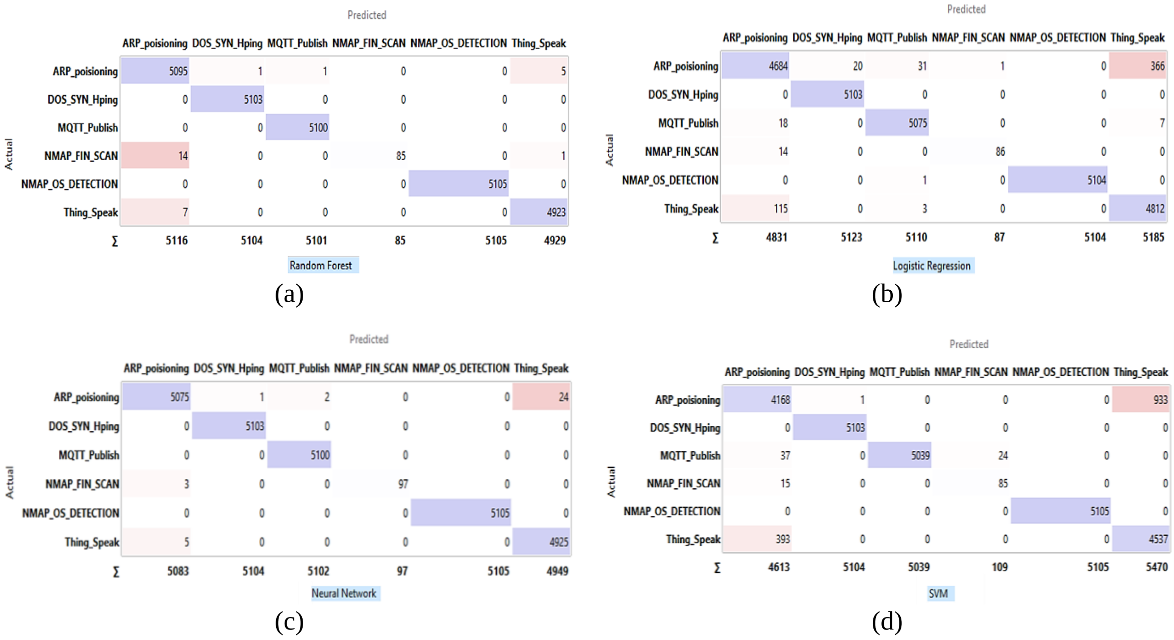
Checking accuracy and efficiency is possible with the performance evaluation methodology. A classifier can be evaluated in several ways. A test set and a train set, each comprising 30% and 70% of the dataset, were used in this investigation. After the data has been trained using the train set, its predicted performance is evaluated using the invisible test set. To further eliminate the issue of overfitting, we employed the cross-validation approach of 10 folds. A comparison was made between the performance of the chosen classifiers; SVM, RF, LR, and ANN are the four ML classification models used in this paper. In ML, a confusion matrix lists the correct and incorrect predictions made by a classification model using a sample of the test dataset. It consists of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN) [40]–[42]. Table 1 demonstrates the confusion matrix, and Table 2 shows classifier performance matrices such as F1-score, recall/sensitivity, accuracy, and precision. The Orange3 data mining tool was used to extract data. By testing the proposed model, a confusion matrix was generated for all classifiers to measure performance using performance matrices. Figure 5 depicts the confusion matrix for all classifiers. The images are divided into four groups: the first represents the confusion matrix for RF as shown in Figure 5(a), the second represents the confusion matrix for LR as shown in Figure 5(b), the third represents the confusion matrix for ANN as shown in Figure 5(c), and the last one represents the confusion matrix for SVM as shown in Figure 5(d).

Table 1. Confusion matrix [43]

		Predicted	
Actual		Congested	Uncongested
	Congested	True positive (TP)	False negative (FN)
	Uncongested	False positive (FP)	True negative (TN)

Table 2. Classifier's performance evaluation [44]

Performance metrics	Equation
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Sensitivity	$\frac{TP}{TP+FN}$
Precision	$\frac{TP}{TP+FP}$
F-measure	$\frac{2*\text{Precision}*\text{Sensitivity}}{\text{Precision}+\text{Sensitivity}}$



Predicted

Actual	ARP_poisioning	DOS_SYN_Hping	MQTT_Publish	NMAP_FIN_SCAN	NMAP_OS_DETECTION	Thing_Speak
ARP_poisioning	5095	1	1	0	0	5
DOS_SYN_Hping	0	5103	0	0	0	0
MQTT_Publish	0	0	5100	0	0	0
NMAP_FIN_SCAN	14	0	0	85	0	1
NMAP_OS_DETECTION	0	0	0	0	5105	0
Thing_Speak	7	0	0	0	0	4923
∑	5116	5104	5101	85	5105	4929

Random Forest

(a)

Predicted

Actual	ARP_poisioning	DOS_SYN_Hping	MQTT_Publish	NMAP_FIN_SCAN	NMAP_OS_DETECTION	Thing_Speak
ARP_poisioning	4684	20	31	1	0	366
DOS_SYN_Hping	0	5103	0	0	0	0
MQTT_Publish	18	0	5075	0	0	7
NMAP_FIN_SCAN	14	0	0	86	0	0
NMAP_OS_DETECTION	0	0	1	0	5104	0
Thing_Speak	115	0	3	0	0	4812
∑	4831	5123	5110	87	5104	5185

Logistic Regression

(b)

Predicted

Actual	ARP_poisioning	DOS_SYN_Hping	MQTT_Publish	NMAP_FIN_SCAN	NMAP_OS_DETECTION	Thing_Speak
ARP_poisioning	5075	1	2	0	0	24
DOS_SYN_Hping	0	5103	0	0	0	0
MQTT_Publish	0	0	5100	0	0	0
NMAP_FIN_SCAN	3	0	0	97	0	0
NMAP_OS_DETECTION	0	0	0	0	5105	0
Thing_Speak	5	0	0	0	0	4925
∑	5083	5104	5102	97	5105	4949

Neural Network

(c)

Predicted

Actual	ARP_poisioning	DOS_SYN_Hping	MQTT_Publish	NMAP_FIN_SCAN	NMAP_OS_DETECTION	Thing_Speak
ARP_poisioning	4168	1	0	0	0	933
DOS_SYN_Hping	0	5103	0	0	0	0
MQTT_Publish	37	0	5039	24	0	0
NMAP_FIN_SCAN	15	0	0	85	0	0
NMAP_OS_DETECTION	0	0	0	0	5105	0
Thing_Speak	393	0	0	0	0	4537
∑	4613	5104	5039	109	5105	5470

SVM

(d)

Figure 5. Confusion matrix of all classifiers (a) confusion matrix of RF classifier, (b) confusion matrix of LR classifier, (c) confusion matrix of ANN classifier, and (d) confusion matrix of SVM classifier

4. RESULT AND DISCUSSION

With a perfect AUC score and excellent accuracy, F-measure, precision, and sensitivity ratings with values of 100%, 99.9%, 99.9%, 99.9%, and 99.9%, the RF model showed remarkable performance by all measures. With an AUC score of 99.8% and values for accuracy, precision, F-measure, and sensitivity around 97.8%, the LR model likewise demonstrated excellent performance. With an AUC score of 100% and accuracy, F-measure, precision, and sensitivity scores of 99.8%, the ANN model also showed exceptional performance. In contrast, the SVM model performed worse, suggesting a potential problem in accurately recognizing positive cases as well as a lower overall prediction accuracy where the AUC score is 99.2% and the accuracy is 92.9%. A comparison of the classifier's performance evaluation is denoted in Table 3 and Figure 6. However, it has been proven that the accuracy shown in this work is better than that of earlier studies. Similar to Khan *et al.* [15], the accuracy rate was 97.13%; the greatest accuracy rate was 98.3% in Pooja *et al.* [18]; and the accuracy rate was 99.0% in Musleh *et al.* [21]. Nonetheless, in this investigation, the IDS system's maximum AUC rate for identifying any attack is 100%. This result satisfies that the RF classifier is the best one because, because of its capacity to overcome noise, handle nonlinear relations, and use high-dimensional information, it has greater classification accuracy. Also, because of its robustness against noise, outliers, and complicated data linkages, the RF classifier is a good option for real-world IoT applications. Its low weight makes it appropriate for devices with limited resources and provides valuable data for identifying issues and status monitoring. The results of the comparison of the classifier's performance evaluation of the proposed model and previous studies are shown in Tables 3 and 4, respectively.

Table 3. Comparison of classifier's performance evaluation

Model	AUC	Accuracy	F-Measure	Precision	Sensitivity
RF	1.000	0.999	0.999	0.999	0.999
LR	0.998	0.978	0.978	0.978	0.978
ANN	1.000	0.998	0.998	0.998	0.998
SVM	0.992	0.929	0.929	0.931	0.929

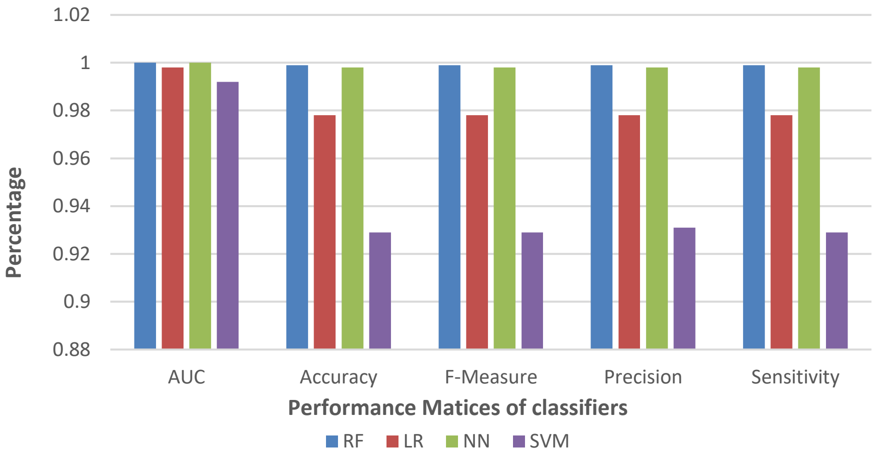


Figure 6. Comparison of classifier's performance evaluation

Table 4. Result comparison of classifier's performance evaluation of previous studies and proposed model

Study/Year	Methods/Model	Performance metrics	Percentage
[11]/2020	Software defined networking (SDN)/network function virtualization (NFV)	Accuracy	99.71%.
[12]/2021	Deep learning model/ResNet-18	Accuracy	98.89%
[13]/2020	J48 decision tree (DT)	Accuracy	99%
[14]/2022	Software defined networking (SDN)/hybrid CNN-LSTM	Accuracy	99.73%
[15]/2021	Deep neural network (DNN), LSTM	Accuracy	97.13%.
[16]/2021	Software defined networking (SDN)	Accuracy	98.5%
[17]/2020	Statistical modeling anomaly detection (SMAD)	True positive rate	96.04%
[18]/2021	LSTM	Accuracy	99.5%
[19]/2022	hybrid DL using LSTM, gated recurrent unit (GRU)	Accuracy	99.5%
[20]/2022	"Looking Back" concept, RF	Accuracy	99.81%
[21]/2023	RF, K-nearest neighbors, SVM and VGG-16	Accuracy	98.3%.
[22]/2021	SVM-binary and multi-class	Accuracy	99.9%
Proposed	RF, ANN, LR and SVM using Orange3 data mining tool	Accuracy	99.9%

5. CONCLUSION

Cybersecurity threats that block authorized IoT network users from using IoT systems' services might take many different forms. The IDS model is therefore suggested to prevent attacks on IoT networks by predicting them to ensure that systems, devices, and data are sufficiently secured and protected. This study aims to provide IDS based on DL and ML approaches to address these problems and stop hackers from successfully attacking IoT networks using various attack data sets. To train the system to identify threats to the IoT, we compared and chose the best dataset in this study. We employed the most well-known ML algorithms (ANN, RF, LR, and SVM) to get the greatest performance for our IDS. Following their training, each of these chosen algorithms completed testing. Finally, a confusion matrix was used to assess and contrast the algorithm's performance matrices including accuracy, F-measure, sensitivity, and precision. Through training RF with 99.9% across all four measures, for ANN the accuracy reached (99.8%), and (97.8%) for LR, and finally in SVM the accuracy reached (92.9%). However, in comparison to other methods like ANN, LR, and SVM, the study shows that the RF classifier is the best at detecting attacks in IoT networks. IoT situations with limited resources in the real world can benefit from RF's resilience, interpretability, and explainability. Future studies ought to combine other security measures with RF-based anomaly detection and use other data mining tools to assess the effectiveness of different classifications and tools. While acknowledging its limits and recommending further investigation, the paper presents the opportunity of RF for IoT security. Prospective areas for future research include verifying results using empirical data, combining RF with other security measures, and investigating distributed methods.

6. FUTURE WORK

Future research aims to verify results using empirical data, combine random forest with security measures, and investigate distributed methods. Researchers will evaluate a random forest-based anomaly detection system using internet of things network data and federated and distributed learning methodologies. On the other hand, the model will be constructed using other data mining tools to find the optimal choice for this issue.

REFERENCES

[1] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, “IoT in smart cities: a survey of technologies, practices and challenges,” *Smart Cities*, vol. 4, no. 2, pp. 429–475, Mar. 2021, doi: 10.3390/smartcities4020024.

[2] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, “Cyber intrusion detection using machine learning classification techniques,” in *Communications in Computer and Information Science*, vol. 1235, Springer Singapore, 2020, pp. 121–131.

[3] E. Hodo *et al.*, “Threat analysis of IoT networks using artificial neural network intrusion detection system,” *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, Yasmine Hammamet, Tunisia, 2016, pp. 1-6, doi: 10.1109/ISNCC.2016.7746067.

[4] S. Tsimenidis, T. Lagkas, and K. Rantos, “Deep learning in IoT intrusion detection,” *Journal of Network and Systems Management*, vol. 30, no. 1, Jan. 2022, doi: 10.1007/s10922-021-09621-9.

[5] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, “A review of performance, energy and privacy of intrusion detection systems for IoT,” *Electronics (Switzerland)*, vol. 9, no. 4, p. 629, Apr. 2020, doi: 10.3390/electronics9040629.

[6] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, “Iot intrusion detection taxonomy, reference architecture, and analyses,” *Sensors*, vol. 21, no. 19, Sep. 2021, doi: 10.3390/s21196432.

[7] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.

[8] R. Chaganti *et al.*, “A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges,” *IEEE Access*, vol. 10, pp. 96538–96555, 2022, doi: 10.1109/ACCESS.2022.3205019.

[9] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, “Distributed denial of service attacks in cloud: state-of-the-art of scientific and commercial solutions,” *Computer Science Review*, vol. 39, Feb. 2021, doi: 10.1016/j.cosrev.2020.100332.

[10] A. Adnan, A. Muhammed, A. A. A. Ghani, A. Abdullah, and F. Hakim, “An intrusion detection system for the internet of things based on machine learning: review and challenges,” *Symmetry*, vol. 13, no. 6, Jun. 2021, doi: 10.3390/sym13061011.

[11] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, “A machine learning security framework for IoT systems,” *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[12] F. Hussain *et al.*, “A two-fold machine learning approach to prevent and detect IoT botnet attacks,” *IEEE Access*, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[13] M. A. Rahman, Y. Al-Saggaf, and T. Zia, “A data mining framework to predict cyber attack for cyber security,” in *2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Nov. 2020, pp. 207–212, doi: 10.1109/ICIEA48937.2020.9248225.

[14] N. Ahuja, G. Singal, D. Mukhopadhyay, and A. Nehra, “Ascertain the efficient machine learning approach to detect different ARP attacks,” *Computers and Electrical Engineering*, vol. 99, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107757.

[15] M. A. Khan *et al.*, “A deep learning-based intrusion detection system for MQTT enabled IoT,” *Sensors*, vol. 21, no. 21, Oct. 2021, doi: 10.3390/s21217016.

[16] P. K. Binu, D. Mohan, and E. M. Sreerag Haridas, “An SDN-based prototype for dynamic detection and mitigation of DoS attacks in IoT,” in *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, Sep. 2021, pp. 1005–1010, doi: 10.1109/ICIRCA51532.2021.9544755.

[17] I. Dutt, S. Borah, and I. K. Maitra, "Immune system based intrusion detection system (IS-IDS): A proposed," *IEEE Access*, vol. 8, pp. 34929–34941, 2020, doi: 10.1109/ACCESS.2020.2973608.

[18] Pooja TS and P. Shrinivasacharya, "Evaluating neural networks using bi-directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, Nov. 2021, doi: 10.1016/j.gltp.2021.08.017.

[19] S. Ullah *et al.*, "HDL-IDS: a hybrid deep learning architecture for intrusion detection in the internet of vehicles," *Sensors*, vol. 22, no. 4, p. 1340, Feb. 2022, doi: 10.3390/s22041340.

[20] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Computers and Electrical Engineering*, vol. 98, Mar. 2022, doi: 10.1016/j.compeleceng.2022.107716.

[21] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, Mar. 2023, doi: 10.3390/jsan12020029.

[22] V. Ivanova, T. Tashev, and I. Draganov, "DDoS attacks classification using SVM," *WSEAS Transactions on Information Science and Applications*, vol. 19, pp. 1–11, Feb. 2022, doi: 10.37394/23209.2022.19.1.

[23] J. Arvidsson, "Real-time internet of things (RT-IOT2022)," *Kaggle*. Accessed: Feb. 22, 2024. [Online]. Available: https://www.kaggle.com/datasets/joebeachcapital/real-time-internet-of-things-rt-iot2022/discussion?sort=undefined.

[24] O. Almomani, "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms," *Symmetry*, vol. 12, no. 6, pp. 1–20, Jun. 2020, doi: 10.3390/sym12061046.

[25] O. Almomani, A. Alsaaidah, A. A. A. Shareha, A. Alzaqebah, and M. Almomani, "Performance evaluation of machine learning classifiers for predicting denial-of-service attack in internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 1, pp. 263–271, 2024, doi: 10.14569/IJACSA.2024.0150125.

[26] D.-W. Chen *et al.*, "A feature extraction method based on differential entropy and linear discriminant analysis for emotion recognition," *Sensors*, vol. 19, no. 7, Apr. 2019, doi: 10.3390/s19071631.

[27] M. Madi, F. Jarghon, Y. Fazea, O. Almomani, and A. Saaidah, "Comparative analysis of classification techniques for network fault management," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 28, no. 3, pp. 1442–1457, May 2020, doi: 10.3906/elk-1907-84.

[28] C. Liu, Z. Gu, and J. Wang, "A hybrid intrusion detection system based on scalable k-means+ random forest and deep learning," *IEEE Access*, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[29] S. Celine, M. M. Dominic, and M. S. Devi, "Logistic regression for employability prediction," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 3, pp. 2471–2478, Jan. 2020, doi: 10.35940/ijitee.c8170.019320.

[30] E. Y. Boateng and D. A. Abaye, "A review of the logistic regression model with emphasis on medical research," *Journal of Data Analysis and Information Processing*, vol. 7, no. 4, pp. 190–207, 2019, doi: 10.4236/jdaip.2019.74012.

[31] M. Elsisi and M.-Q. Tran, "Development of an IoT architecture based on a deep neural network against cyber attacks for automated guided vehicles," *Sensors*, vol. 21, no. 24, Dec. 2021, doi: 10.3390/s21248467.

[32] L. Chen, S. Li, Q. Bai, J. Yang, S. Jiang, and Y. Miao, "Review of image classification algorithms based on convolutional neural networks," *Remote Sensing*, vol. 13, no. 22, Nov. 2021, doi: 10.3390/rs13224712.

[33] L. Zhang, Z. Li, Y. Hu, C. Smith, E. M. G. Farewik, and R. Wang, "Ankle joint torque estimation using an EMG-driven neuromusculoskeletal model and an artificial neural network model," *IEEE Transactions on Automation Science and Engineering*, vol. 18, no. 2, pp. 564–573, Apr. 2021, doi: 10.1109/TASE.2020.3033664.

[34] D. Devikanniga, A. Ramu, and A. Haldorai, "Efficient diagnosis of liver disease using support vector machine optimized with crows search algorithm," *EAI Endorsed Transactions on Energy Web*, vol. 7, no. 29, p. 164177, Jul. 2020, doi: 10.4108/EAI.13-7-2018.164177.

[35] N. H. Putri, M. Fatekurohman, and I. M. Tirta, "Credit risk analysis using support vector machines algorithm," *Journal of Physics: Conference Series*, vol. 1836, no. 1, Mar. 2021, doi: 10.1088/1742-6596/1836/1/012039.

[36] A. M. Elshewey, M. Y. Shams, N. El-Rashidy, A. M. Elhady, S. M. Shohieb, and Z. Tarek, "Bayesian optimization with support vector machine model for Parkinson disease classification," *Sensors*, vol. 23, no. 4, p. 2085, Feb. 2023, doi: 10.3390/s23042085.

[37] M. A. Almaiah *et al.*, "Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels," *Electronics (Switzerland)*, vol. 11, no. 21, p. 3571, Nov. 2022, doi: 10.3390/electronics11213571.

[38] A. Arabiat and M. Altayeb, "Assessing the effectiveness of data mining tools in classifying and predicting road traffic congestion," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 2, pp. 1295–1303, May 2024, doi: 10.11591/ijeecs.v34.i2.pp1295-1303.

[39] "Orange data mining library," *Orange Data Mining*. Sphinx and Alabaster, Accessed: Jun. 06, 2024. [Online]. Available: https://orange3.readthedocs.io/projects/orange-data-mining-library/en/latest/

[40] Zakoldaev D. A. *et al.*, "Machine learning methods performance evaluation," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2664–2666, Apr. 2021, doi: 10.17762/turcomat.v12i2.2284.

[41] A. Arabiat and M. Altayeb, "An automated system for classifying types of cerebral hemorrhage based on image processing techniques," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 2, pp. 1594–1603, Apr. 2024, doi: 10.11591/ijece.v14i2.pp1594-1603.

[42] A. E. Maxwell, T. A. Warner, and L. A. Guillén, "Accuracy assessment in convolutional neural network-based deep learning remote sensing studies—part 1: Literature review," *Remote Sensing*, vol. 13, no. 13, Jun. 2021, doi: 10.3390/rs13132450.

[43] M. Altayeb and A. Arabiat, "Crack detection based on mel-frequency cepstral coefficients features using multiple classifiers," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3332–3341, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3332-3341.

[44] S. S. S. A. Palma, M. N. dos Reis, and R. Gonçalves, "Tomographic images generated from measurements in standing trees using ultrasound and postprocessed images: methodological proposals for cutting Velocity, interpolation algorithm and confusion matrix metrics focusing on image quality," *Forests*, vol. 13, no. 11, p. 1935, Nov. 2022, doi: 10.3390/f13111935.

BIOGRAPHIES OF AUTHORS

Areen Arabiat earned her B.Sc. in computer engineering in 2005 from Al Balqaa Applied University (BAU), and her MSc in intelligent transportation systems (ITS) from Al Ahliyya Amman University (AAU) in 2022. She is currently a computer lab supervisor at the Faculty of Engineering/Al-Ahliyya Amman University (AAU) since 2013. Her research interests are focused on the following areas: machine learning, data mining, image processing and artificial intelligence. She can be contacted at email: a.arabiat@ammanu.edu.jo.

Muneera Altayeb obtained a bachelor's degree in computer engineering in 2007, and a master's degree in communications engineering from the University of Jordan in 2010. She has been working as a lecturer in the Department of Communications and Computer Engineering at Al-Ahliyya Amman University since 2015, in addition to her administrative experience as assistant dean of the Faculty of Engineering during the period (2020-2023). Her research interests focus on the following areas: digital signals and image processing, machine learning, robotics, and artificial intelligence. She can be contacted at email: m.altayeb@ammanu.edu.jo.