RESEARCH PAPER

Performance Evaluation of Machine Learning Models for Detecting Vulnerabilities in Internet of Things Network.

Anand TR[1*], Mohana Priya T[2], Poorana Senthilkumar S[3], Vijayalakshmi P S[4], Thirunavukkarasu V[5],Rajesh Kanna R[6]

[1]*Department of Computer Technology, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India*
[2,5,6] *Department of Computer Science, CHRIST University, Bangalore, Karnataka, India*
[3,4]*Department of Computer Applications, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India*

ABSTRACT
Security threats and attacks are a growing concern in the field of Internet of Things (IoT) infrastructure. Internet-based automated network application models are used across various domains; commensurately, different security vulnerabilities and anomaly attacks are also increased at the same level. These attacks could cause failures in IoT infrastructure and network systems. In the modern world, Machine Learning (ML) models support various predictive analyses, providing more accurate results for future forecasting in various fields. In this article, we compare existing classical Machine Learning (ML) algorithms supported by Artificial Intelligence (AI) to evaluate and predict the performance and accuracy of different vulnerabilities in IoT infrastructure. We considered and compared the results of Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN) using publicly available datasets. Through this evaluation, we obtained an accuracy of 99.4% from DT, RF, and ANN. Additionally, RF demonstrated a highest accuracy of F1 is 0.994 and lowest STD variance is ±0.014 than compared models in the selected dataset.

Keywords: Attacks and detection; Dataset, Internet of Things, Machine Learning, Vulnerabilities..
How to cite this article: Anand TR, Priya MT, Senthilkumar PS, Vijayalakshmi PS, Thirunavukkarasu V, Kanna RR.., Performance Evaluation of Machine Learning Models for Detecting Vulnerabilities in Internet of Things Network...Int J Drug Deliv Technol. 2026;16(2s): 627-638; DOI: 10.25258/ijddt.16. 627-638
Source of support: Nil.
Conflict of interest: None

INTRODUCTION

The growth and demand for automated and autonomous networks in various domains of the IoT network model are creating day-to-day challenges for security systems. The IT sector is increasingly data-driven, automating people's daily activities across various fields. More research applications and proposals are being presented on ML and the IoT for their automated operations. The combined system of ML and IoT technology is advancing the IT sector to the next level in everyday life.

The growing complexity of real-time data collection in IoT models is increasing security vulnerabilities, and security breaches have become common phenomena in IT-enabled fields. The ML-based prediction models are used in the following fields, such as: the medical field, ECG analysis, disease detection, and automated pathological models for brain signal analysis contributes ML-based prediction solutions. In agriculture, ML is used for tasks like leaf disease detection, soil and seed quality estimation, and determining irrigation needs. These complex tasks are automated to minimize farmers' losses and reduce human effort while ensuring high-quality production and prediction [1]. Similarly, the automobile industry utilizes ML for predictive maintenance, safety and other applications [2]-[3]. Beyond these fields, many industries are adopting ML for prediction and IoT for automating data collection to support these predictions. As a result, IT-driven industries are increasingly integrating these two technologies, making them indispensable.

In IoT infrastructure, communication and broadcasting data models use wireless mediums, which are more susceptible to targeted attacks. The general form of security measures in IoT infrastructure are limited to the local domain or node level, and these security concerns cannot be effectively expanded to cover larger areas, which can devastate and affect IoT system setups [4].

IoT network architecture lack proper authentication mechanisms, and data breaches and poor security standards are common in many applications. For example, in 2016, the Mirai botnet attack remotely controlled bots and affected major applications like Twitter and Netflix. Similarly, in 2021, vulnerabilities were found in thousands of smart cameras against Domain Name System (DNS) providers and affected millions user applications [5]-[8].

Thenceforth, higher security is required to protect IoT models from attackers. Many security measures have different effects on the vulnerabilities in IoT network setups. Any classified form of an IoT components and data are the backbone and confidential elements for the proper execution of IoT systems. Entry points, such as backdoors, can create security vulnerabilities and potentially lead to the breakdown of IoT models. For example, governments, business organizations, and private agencies are currently working on smart application models that handle confidential and important data. Machine Learning prediction models systematically assess risks to data

**Author for Correspondence: Anand TR*

protection in modern systems, especially those handling various IoT datasets and data models, or both. These models consider the entire ML life cycle and different ML architectures. The adoption of ML to solve an extensive range of real-life problems has highly led to the collection and processing of large volumes of data, including sensitive information. Privacy-enhancing technologies are often recommended to protect network data and ensure reliability, as required by traditional and present IoT infrastructure model on data protection through AI [5]. However, standalone IoT applications are insufficient to guarantee high-quality data protection. The utilization of an ML-based model framework, privacy and confidentiality risks in network data can be better addressed. These models help identify, assess, and mitigate privacy vulnerabilities, enabling the implementation of countermeasures to prevent data breaches in machine learning environments [9]-[10].

The primary goal of this ML model and IoT real-time dataset analysis is to develop a smart, reliable, and privacy-focused data protection system for IoT-based infrastructure. This system can prevent and detect network data vulnerabilities and attacks, helping to avoid network failure cases in IoT infrastructure.

Further, analysis, evaluation and comparison with other recent related works will be carried out in Section 2, which provides an overview of related research articles and on IoT infrastructure attacks and detection techniques. Section 3 describes the selected dataset material and method, followed by Section 4, which explains the experimental setup and results of the considered models. Finally, Section 5 presents the conclusion and future scope of this analysis.

RELATED RESEARCH WORKS

This related work section presents a several associated works surveys on the security threats prediction related with ML and IoT systems datasets. The principal security risks are examined, along with the recent proposed countermeasures. We highlight primary contributions made in the field, and also identify important of the related to that further investigation and in-depth analysis.

The IoT has led to the rapid growth of connected devices, but this growth also brings security challenges, especially due to the emergence of zero-day cyberattacks [11]. Many studies have explored network-based intrusion detection systems (NIDS) for IoT security, with deep learning (DL) techniques showing promise in improving detection accuracy and reducing false alarm rates (FAR). A Varity of deep learning models, such as deep neural networks (DNN), recurrent neural networks (RNN), convolutional neural networks (CNN), and their variants like Long-Short-Term - Memory (LSTM) and Gated-Recurrent-Units (GRU), have been proposed for anomaly detection [12]. Comparative studies show that DNN-based NIDS outperform traditional models, with improved detection accuracy (0.57–2.6%) and a reduction in FAR (0.23–7.98%). Feature selection, particularly using the 16–35 best numerical features, reduces model complexity without significant performance loss. This incorporation of both categorical and numerical data features further enriched the accuracy. Moreover, these improvements, challenges remain in handling imbalanced feature datasets and real-time data processing will need on continued research.

In the background of Industry 4.0, anomaly node detection in machine vision systems plays a vital role in enhancing smart-industrial requirements and efficiency, adoptability and innovation [13]. These authors present a machine vision system designed for identifying and classifying anomalies in modern advanced gearbox assembly models. The system operates the Volatile Fatty Acid (VFA) methodology, which combines fuzzy entropy and Euclidean fuzzy similarity measures to facilitate nonlinear transformation through deterministic functions. This approach creates a reliable and realistic anomaly detection model. The measurement of evaluation and assessment of this system was experimented in a complex security scenario where cybercriminals attempted to modify production machine, a change that was not detected by other sensor nodes in the system. The associative of advanced machine vision and fuzzy logic model implementation practice, the system obtains a high success rates in anomaly detection. This work also recommends extension of system's functionality by employing intuitive fuzzy logic and dissimilarity measures, which would further help the sensitivity and detection of the attacks. Further, the use of protecting VFAs for anomaly detection in future work could enhance the system's robustness.

The proposed model provides an advanced security solution to a critical attack problem in information systems by ensuring high truthfulness and reliability [14]. The AI algorithm embedded in the methodology, which accelerates the learning rate, allowing for faster convergence in smart-industrial models. This system's self-adaptation and self-learning features enable it to identify and maintain the primary characteristics of complex patterns, leading to accurate and timely predictions relevant to smart industrial setup environments. The model enhances prediction by the concept of eliminating the variability attributed to industrial sensitive data, effectively differentiative minute details among complex data. The system model provides intelligent correlation algorithms and machine learning structures to enhance reliable predictions, which typically improve categorization rates and minimize the probability of wrong decisions. Given the rapid generation of extensive quantities of industrial data, classical learning algorithms generally fails to manage stream data. The proposed model, provides notable reliability in predicting data shifts, with a low "mutation" rate, assure the discovery of local extremes and enabling better model integration in dynamic environments.

Cybersecurity remains a major challenge in the employment of IoT systems, particularly counter to cyber-attacks. To address this issue, [15] introduces a new IoT architecture that leverages enriched ML techniques to detect cyber-attacks and monitor the status of induction motors with notable accuracy. The proposed system utilizes the CONTACT Element platform for IoT to provide real-time, economical, and secure monitoring of motor status through communication channels and internet connections. The IoT platform automatically visualizes detected cyber-attacks as fraudulent data on the dashboard, enhancing the system's

security. Various experimental scenarios with data acquisition validate the proposed IoT topology's performance, confirming its ability to effectively visualize motor issues and cyber-attacks with great accuracy. Notably, the architecture incorporates the Random Forest algorithm, achieving 99.03% accuracy in detecting motor faults due to vibration under industrial conditions, outperforming other ML models. The proposed IoT platform is also characterized by low latency, ensuring quick detection and visualization of motor faults and cyber-attacks.

The author [16] evaluates eight ML and DL models, including DT, KNN, RF, SVM, LR, Gradient Boosting (GB), Naïve Bayes (NB), and Artificial Neural Network (ANN), using the CIC IoT Dataset 2022. The dataset, preprocessed with CICFlow-Meter to extract over 80 statistical features, was balanced using sampling techniques. Recursive Feature Elimination (RFE) identified critical features like Pkt Len Max, enabling effective attack detection. Experiments using two feature sets (six and three features) showed Gradient Boosting outperformed other models, achieving accuracies of 95.94% and 95.28%. The model excelled in detecting Flood and RSTP brute-force attacks. This research underscores the performance of ML and DL methods in enhancing IoT network security and protecting sensitive data.

In recent work, the authors proposed a model an AI-based intrusion detection system (IDS) accommodating advanced feature selection techniques combining fuzzy logic and genetic algorithms (GA). The approach integrates bio-inspired optimization methods, such as Intelligent Water Drop (IWD) and Biogeography-Based Optimization (BBO), to enrich feature selection [17], [18]. A feed-forward fuzzy water drop network (FWDNN) was implemented for successful intrusion detection and attack classification. This proposed model was evaluated on real IoT network datasets and CICIDS-2017, the result demonstrates superior performance compared to existing models across various evaluation key metrics. This model highlights its efficiency in detecting malicious activities in an IoT networks.

Another latest research work-based intrusion detection systems (IDS) integrated in resource-constrained IoT environments [19]. The research work proposed an intelligent IDS integrating proportion minimized through Principal Component Analysis (PCA) and machine learning techniques. Using the dataset UNSW-NB15, and this model achieved noteworthy detection performance, addressing challenges like labeled data and communication overhead in IoT networks. PCA-selected components integrated with classifiers such as XgBoost and CatBoost shows an exceptional accuracy of 99.99%. This approach effectively enriches IoT security in smart cities and healthcare applications. Future directions required on the integration of deep learning models for improved traffic classification.

The authors proposed an AI-driven IDS architecture for securing the Internet of Vehicles (IoV) [20]. Deep learning-based classifier engines (DLEs) were deployed on Multi-access Edge Computing servers to classify vehicles based on possible attack types using vehicle-generated messages. Among the classification techniques explored, sequence-image-based classification using CNNs outperformed other models [21]. The work addressed major cybersecurity attack types in IoV scenarios, with future plans to include additional misbehavior types, such as vehicular sensor malfunctions and faulty data transmission, in next-generation intelligent transportation systems.

The authors highlight an advanced IDS designed for IoT networks using artificial intelligence algorithms to combat cybersecurity threats [22]. The system considered KNN, Linear Discriminant Analysis (LDA), CNN, and convolutional long short-term memory networks (CNN-LSTM) to detect MQTT protocol-based intrusions. Using a Kaggle-sourced dataset injected with attacks like brute-force, flooding, malformed packets, SlowITe, and normal packets, the system demonstrated high performance. The CNN-LSTM model achieved 98.94% accuracy, surpassing KNN (80.82%) and LDA (76.60%), showcasing its effectiveness in safeguarding IoT communication via MQTT protocols.

The authors proposed an anomaly detection model proving deep neural networks (DNN) enhanced with the chicken swarm optimization (CSO) algorithm to effectively detection mechanisms for securing networks [23]. Evaluated on the UNSW-NB15 dataset, the model achieved 94.85% accuracy and a 96.53% detection rate, outperforming techniques like GA-NB, GSO, and PSO. The DNN-CSO model demonstrates high efficiency in identifying anomalies, making it suitable for securing IoT networks.

The growing field of IoT network adoption has led to increased network traffic, the traditional attack detection methods will be insufficient [24]. These authors proposed an architecture model for detecting malicious node in IoT network traffic using supervised machine learning algorithms: SVM, Gradient Boosted Decision Trees (GBDT), and RF. Evaluated on the NSL-KDD dataset, the RF algorithm recorded the highest accuracy of 85.34% and outperformed other metrics of specificity and prediction time.

The obtained results confirm that supervised ML techniques effectively identify malicious traffic in IoT network. In future the same proposed work can be expanded by exploring new IoT devices, malware-infected data, and advanced technologies for enhanced IDS. The Table 1. summarizes key aspects of the related works from [12] to [24], comparing methods, results, and limitations

Table 1. Summary of Related Works

Author(s)	Key Focus	Methods/Techniques Used	Dataset Used	Results Achieved	Limitations

[12]	Anomaly detection	False rate alarm (FRA) with DL	Balanced dataset	Improved detection accuracy	Not considered imbalanced and real time dataset
[13]	Abnormality detection in machine vision for Industry 4.0	VFA methodology, fuzzy entropy, Euclidean fuzzy similarity, machine vision techniques	Cybersecurity scenario	High success rates in anomaly detection; potential for cybersecurity applications	Limited to specific industrial contexts; scope for enhancing fuzzy logic methodologies
[14]	Timely predictions and elimination of variable attribute for industrial models	Intelligent correlation algorithms and machine learning	Industrial sensitive data	Reliability in shifting and mutation rate.	Limited Industrial datasets
[15]	IoT intrusion detection for induction motor monitoring	Machine learning techniques, Random Forest, IoT architecture	CONTACT Element IoT	Achieved 99.03% accuracy in detecting motor faults; reduced latency and improved visualization	Limited scenarios evaluated; potential for expansion with other ML techniques and datasets
[16]	Cyberattack detection using AI models	ML and DL techniques for flood and brute-force cyberattacks	CIC IoT Dataset 2022	Achieved 95.94% accuracy using Gradient Boosting model; high performance with both feature sets	Dataset imbalance; further testing required for generalization to other attacks
[17]-[18]	IDS based on fuzzy and genetic algorithms [15]	Fuzzy and genetic algorithms, intelligent water drop (IWD), biogeography-based optimization (BBO), neural network	IoT and CICIDS-2017 dataset	BBOKNN model outperformed others in terms of evaluation metrics	No specific analysis of real-world IoT environments; limited to dataset-driven results
[19]	ML-based IDS in resource-constrained IoT	Feature dimensionality reduction, PCA, XgBoost, CatBoost, KNN, SVM, QDA, NB algorithms	UNSW-NB15 dataset	Achieved 99.99% accuracy with PCA-XgBoost and PCA-CatBoost models	Focus on limited dataset; requires further optimization for real-time IoT systems

[20]-[21]	AI-based intrusion detection in IoV	Deep learning, CNN for sequence-image-based classification, edge computing servers	IoV network messages	CNN performed best among models, used to detect vehicle attack types	Future work to cover all types of misbehavior; requires expansion for ITS scenarios
[22]	IoT intrusion detection based on AI algorithms	KNN, LDA, CNN, CNN-LSTM for MQTT protocol IoT intrusion detection	Kaggle dataset	CNN-LSTM achieved 98.94% accuracy; good detection of malicious IoT traffic	Need for broader attack types; limited by dataset scope and validation
[23]	IoT security using anomaly detection with DNN and CSO	DNN for anomaly detection, chicken swarm optimization (CSO) for optimization	IoT dataset	94.85% accuracy; model outperformed GA-NB, GSO, and PSO methods	Limited to dataset-specific scenarios; needs improvement for more complex IoT environments
[24]	Malicious network traffic detection for IoT	SVM, GBDT, RF classification methods for detecting malicious network traffic	NSL-KDD dataset	RF algorithm achieved 85.34% accuracy for malicious traffic detection	Limited traffic types analyzed; further exploration into additional IoT datasets and technologies

The related works highlight the critical role of ML in enhancing IoT network security against evolving cyber threats. Various approaches, including deep learning, feature selection algorithms, and ensemble methods, have demonstrated improved anomaly detection and intrusion prevention. Several frameworks utilized advanced techniques such as PCA, fuzzy algorithms, and neural networks, achieving accuracy rates exceeding traditional methods. However, many existing works focus on introducing new methodologies without thoroughly evaluating the foundational impact of standard ML models. Additionally, some studies did not emphasize large datasets, limiting the scalability and generalizability of their solutions. Most proposed models failed to surpass 90% accuracy consistently, underscoring the need for more robust frameworks. Future efforts should prioritize leveraging large-scale datasets and optimizing ML models to achieve higher detection accuracy and scalability while maintaining simplicity and computational efficiency in resource-constrained IoT environments.

MATERIALS AND METHODS

This section explores and describes the selected dataset for this evaluation, along with classical ML models applied to predict the best model.

Dataset

The overall analysis configuration setup consists of different levels of independent phases. Figure. 1 presents an overview of the system's phases. The initial phase involves data collection and dataset examination. In this phase, suitable real-time data is systematically selected, collected and examined to observe the data types and attributes. The selected dataset contains both normal IoT data patterns from various IoT applications and different type of attacks.

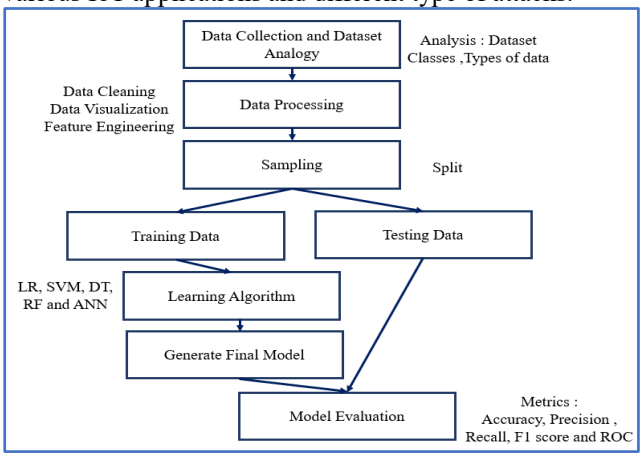

Figure 1. Workflow Phases

The next process of converted the data into feature vector, the data processing implementation is required on the collected dataset, it consist of cleaning, visualization, feature engineering and vectorization on the data. These feature vectors data 100% is divided into 70 ratio data for training and 30 ratio data testing. The training data is used in the ML model algorithm, and final model is developed to find the optimized model [25].

Dataset selection and description

The publicly available dataset was selected from the Kaggle platform [26]. This dataset was virtually created in an IoT environment, producing synthetic data, and was posted by Pahl et al. The selected dataset contains 357,952 sample records with 13 features, consisting of 347,935 healthy data frequencies and 10,017 affected data frequencies, classified into 8 different categories. The 13 features of the dataset are listed in Table 2. In this dataset, the data types of the features are nominal (object type), except for the timestamp feature, which is discrete (Int64). Table 3 provides the exact frequency count of different anomaly attacks from the entire dataset.

Data preprocessing

The first task in data analysis is to feed the dataset into a classifier in the machine learning exploratory process [27]. To examine the missing data, the 'Accessed Node Type' (ANT) column, which contains categorical values, and the 'Value' column, which contains continuous values, were observed. The ANT column contained 148 'Not a Number' (NaN) entries. Removing and eliminating these 148 entries would result in the loss of valuable data. Therefore, these NaN recorded entries were replaced with the value 'Malicious' Similarly, missing data in the 'Value' feature were replaced using a similar methodology, where continuous values were substituted with meaningful values such as '0.0', '1.0', '20.0', etc. [28]

Table 2. Dataset Features

S.No	Features	Data Types
1	Source_ID	nominal-Obj-type
2	Source_Address	nominal-Obj-type
3	Source_Type	nominal-Obj-type
4	Source_Location	nominal-Obj-type
5	Destination_Service_Address	nominal-Obj-type
6	Destination_Service_Type	nominal-Obj-type
7	Destination_Location	nominal-Obj-type
8	Accessed_Node_Address	nominal-Obj-type
9	Accessed_Node_Type	nominal-Obj-type
10	Operation	nominal-Obj-type
11	Value	nominal-Obj-type
12	Timestamp	discrete-Int-64
13	Normality	nominal-Obj-type

Table 3. Attacks frequency

S.No	Attacks	Count
1	Denial of Service	5,780
2	Scan	1,547
3	Malicious Control	889
4	Malicious Operation	805
5	Spying	532
6	Data Type Probing	342
7	Wrong Setup	122
Total		10,017

In most related works, no feature selection or advanced machine learning approach has been applied. In the feature engineering process, it is essential to identify the types of features in the dataset, as the selected dataset contains both numerical and categorical data. The numerical data includes discrete and continuous values, while the categorical data can be grouped into nominal and ordinal categories. According to the selected dataset from Table 1, the 'Timestamp' and 'Value' features are not considered in this work.

The next crucial step is converting nominal type features into vectors, as categorical values can be transformed into vectors in various ways. Label encoding (numerical number) and one-hot encoding (0s and 1s) are two prominent methods for numerical values to fit the data into ML models. In this work, we applied label encoding to the selected dataset because most of the features were of the same type [29]. Additionally, using one-hot encoding would result in more dimensions, making it harder to fit into machine learning algorithms.

Theoretical proof

AI machine learning algorithms are a set of mathematical models and computational techniques used for analysis, where they predict output values from given input data [30]. Various algorithms can be applied in machine learning-based prediction models across different fields and datasets. The following subsections provide theoretical explanations of these machine learning algorithms.

Logistic Regression (LR)

LR, also called the logit function, is a type of classification model used when the response variable is categorical [31]. The fundamental idea behind logistic regression is to analyze the relationship between features and the probability of a particular predicted outcome. LR uses the sigmoid function to map predictions to probabilities [32].

LR is a discriminative model that relies on the independent variables in the given dataset [29]. In our case, we considered four following features to predict the value,

Let $X = X_0, X_1, ..., X_{n-1}$ represent the distinct features, $W = W_0, W_1, ..., W_{n-1}$ represent the weights, and $b = b_0, b_1, ..., b_{n-1}$ represent the biases, while $C = c_0, c_1, ..., c_7$ represents the 8 classes. The equation for the estimation is specified as follows in Equation. (1).

$$Predicted\ Value(C) = \frac{1}{1+exp^{-(W.X+b)}} \quad (1)$$

Support Vector Machine (SVM)

Like LR, SVM is a supervised learning model pre-owned for both linear and non-linear classification, as well as outlier detection and regression [33]. Compared to other models, SVM is particularly suitable for non-linear data. Let x_i represent the input, c_i represent the class, and α_i represent the Lagrange multiplier values. The weight vector W estimation can be calculated using the following Equation. (2) to find the optimal hyperplane.

$$W = \sum_{i=0}^{n-1} x_i \alpha_i c_i \quad (2)$$

Where W is the weight vector that defines the hyperplane.
α_i are the Lagrange multipliers (non-negative values).
c_i are the class labels (usually + 1 or − 1 for binary classification).
x_i are the input data points.
n is the number of training samples.
The dual formulation uses Lagrange multipliers
α_i to convert the problem into a maximization problem. The dual objective function is using the following Equation. (3):

$$Maximize\ \alpha_i \sum_{i-0}^{n-1} \alpha_i - \frac{1}{2} \sum_{i=0}^{n-1} \sum_{i=0}^{n-1} \alpha_i \alpha_i c_i c_i (x_i, x_j) \quad (3)$$

Decision Tree (DT)

A DT is a popular supervised learning algorithm mostly applied for classification and regression tasks, capable of predicting class labels by incrementally splitting data based on feature values [34]. The tree begins at the root node, representing the entire dataset, and splits into branches according to conditions that maximize valuable information gathering or minimize impurity. Each decision node tests a specific attribute, while leaf nodes represent the final class labels or outcomes. This process involves recursively partitioning the data based on attribute values until a stopping criterion is met. DT handle both numerical and categorical data effectively and require minimal preprocessing. The splitting criterion often uses Information Gain, which is calculated using Equations (4) and (5):

$$Information\text{-}Gain = H(parent) - \sum_{i=1}^{k} \frac{|child_i|}{|parent|} . H(chilld_i) \quad (4)$$

Where H is $H = - \sum_{i=1}^{k} p_i log_2(p_i)$ (5)

Random Forest (RF)

RF is a powerful supervised learning algorithm that highly follows both classification and regression tasks in machine learning. It supports the principles of composite learning, where multiple decision trees are combined to identify the class or value of a given dataset [35]. This modern approach makes RF particularly effective solution for complex problems which includes classified, uncorrelated datasets. The primary concept of using multiple trees allows RF to attain higher accuracy, reduce overfitting, and handle huge datasets efficiently. It also requires minimal training time and enabling models to be developed very easily and quickly compared to other existing algorithms. A main feature of RF is the use of out-of-bag (OOB) sample datasets for cross-validation and finalizing predictions, which enhances model accuracy and helps prevent overfitting.

Artificial Neural Network (ANN)

ANNs are a sub-field of artificial intelligence encouraged by the structure and functioning of the human brain [36]. ANNs consist of interlinked neurons connected to each other via weighted connections, which represent the strength and type of relationships [37]. They are especially suitable for handling nonlinear datasets and are capable of recognizing complex patterns same as how human nerve cells process information. The working approach of ANNs involves three layers: input, hidden, and output, while also performing parallel and distributed information processing learned from training samples. Although optimizing errors in ANNs takes longer than with other techniques, their ability to adapt to data and learn through real-time operations, adaptive learning, and self-organization makes them highly advantageous. These networks excel in solving complex problems through pattern recognition and generalization.

In a non-linear dataset, several popular types of activation functions can be used to process individual input samples. After this, the softmax function is applied to compute the initial predicted values. The softmax function calculates the predicted probability for each class as follows the Eq. (6).

$$pp_i = \frac{e^{zi}}{\sum_{j=1}^{n} e^{zi}} \quad (6)$$

Here, pp_i represents the predicted probability for class i, and zi is the input to the softmax function. These predicted values, along with the true values, are then used to compute the loss function, which helps update the weights across the entire neural network architecture.

EVALUATION AND RESULT ANALYSIS

To evaluate the performance of the classical model and ensure its suitability for the given problem, the following performance metrics are used for a comprehensive assessment:

Confusion Matrix: A tabular representation that presents the true positive, true negative, false positive, and false negative values, providing insight into the classification performance.

Accuracy: Gives the overall correctness of the model's predictions, calculated as the ratio of accurately predicted instances to the given total instances [38].

Precision: Calculates the measures of positive predictions by identifying the proportion of rightly predicted positive instances out of all instances predicted as positive.

Recall: This metric measures the ability of the model to perfectly identify positive instances, computed as the ratio of true positives to the total actual positive instances.

F1 Score: The mean values of Precision and Recall, offering a balanced measure of the two metrics. It is specifically valuable when there is an uneven class distribution models [39].

Receiver Operating Characteristic (ROC) Curve: A graphical representation that illustrates the diagnostic

ability of a binary classifier by plotting the true positive rate (Recall) against the false positive rate at various threshold settings [39].

Experimental Configuration

The experiment was conducted on a LENOVO 81FS desktop running Microsoft Windows 11 Pro (Version 10.0.22631, Build 22631) with an AMD64 Family 21 processor (~2300 MHz), 4 GB RAM, and a virtual memory capacity of 6,112 MB. The system utilized Pandas and NumPy for data preprocessing, Matplotlib and Seaborn for visualization, and Scikit-learn and Keras for data analysis and model training. This setup provided sufficient resources for handling the dataset and executing the experiments effectively.

Result Analysis

In this section, the machine learning techniques discussed earlier were applied to the selected dataset. Five-fold cross-validation was performed using all of these techniques [31]. Instead of standard cross-validation, five-fold cross-validation addresses the probable issue of class imbalance, because each fold provides the class distribution and ensures balanced representation of the majority and minority classes in the given dataset through stratification [40].

The results showed that RF and ANN outperformed then other models in both the training and testing datasets. The performance of DT was significantly similar to that of RF and ANN in terms of training accuracy. However, when tested on the testing data, DT showed considerable deviation and performed poorly, although it delivered consistent results across the subsequent three folds. SVM and LR performed worse compared to the other models during training. Interestingly, in the first fold of the testing phase, both SVM and LR performed better than the other techniques, with LR showing superior performance. However, in the next three folds, both SVM and LR exhibited poorer results than the other models. As per 70:30 ratio the training and testing obtained accuracy result is presented in the Figure. 2 (a) and (b). The Figure 3. shows the training and test data metrics comparison.

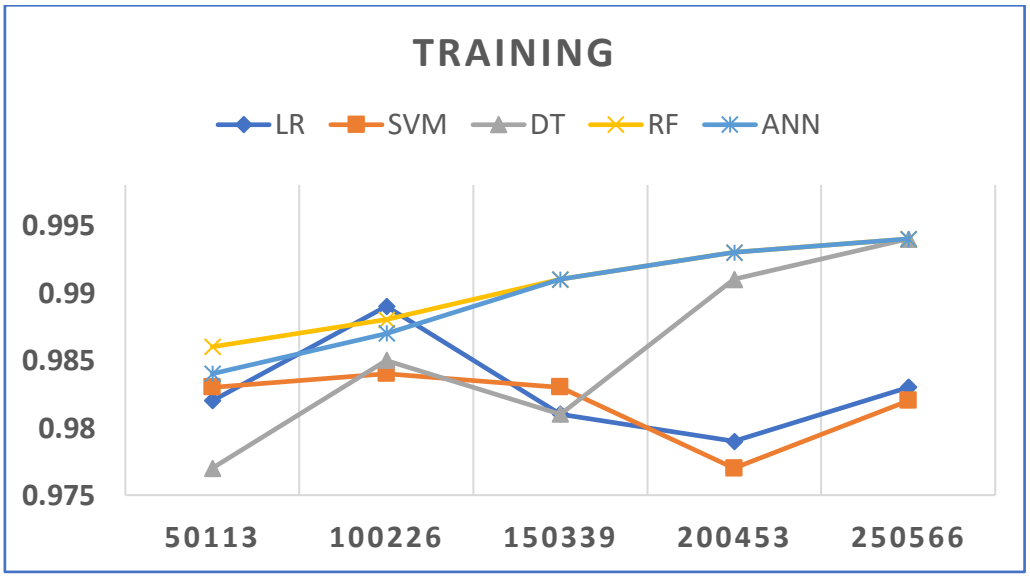

Figure 2. (a) Fold-Cross Validation Training data accuracy.

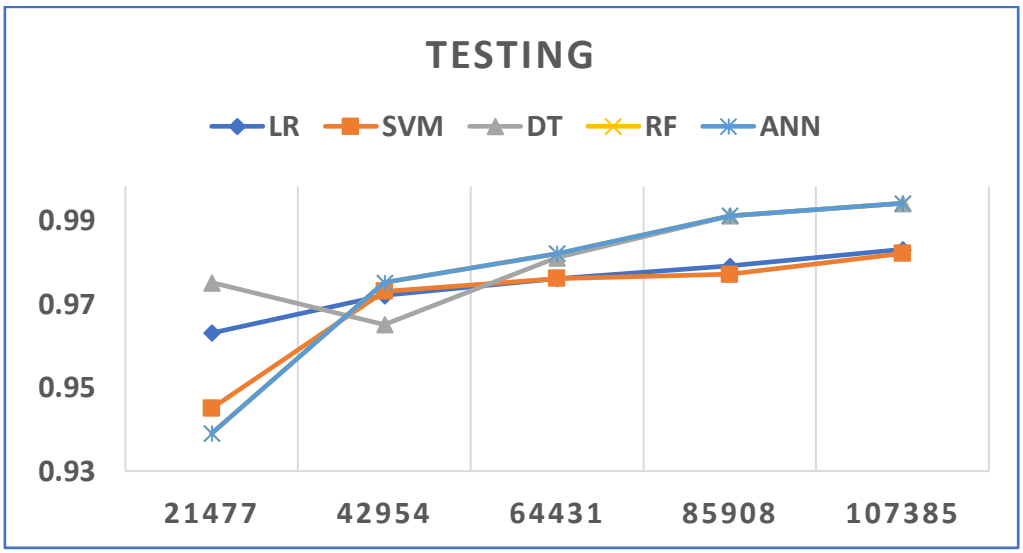

Figure 2. (b) Fold-Cross Validation Testing data accuracy.

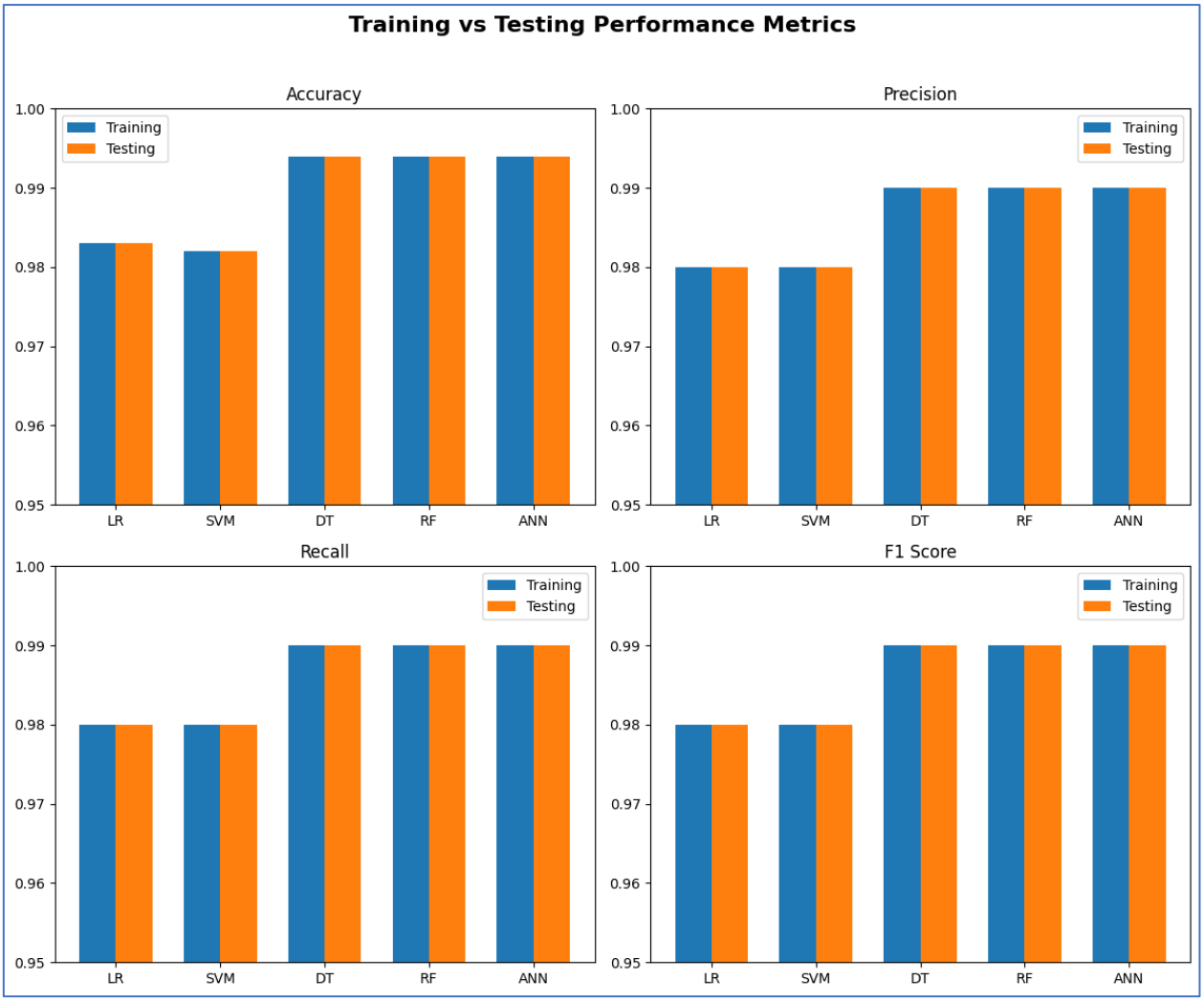

Figure 3. Training and testing metrics performance

The Tables 4 and 5 present the different evaluation metrics for various techniques trained and tested on the dataset. It can be observed that DT, RF, and ANN show high accuracy, precision, recall, and F1 score. Although LR and SVM perform well on our selected dataset, they do not have as significant an impact as the other classifiers

Table 4. Evaluation Metrics of Training Dataset

Metrics	Accuracy	STD (+/-)	Precision	Recall	F1 Score
LR	0.983	0.0012	0.98	0.98	0.98
SVM	0.982	0.0015	0.98	0.98	0.98
DT	0.994	0.00081	0.99	0.99	0.99
RF	0.994	0.00081	0.99	0.99	0.99
ANN	0.994	0.0013	0.99	0.99	0.99

Table 5. Evaluation Metrics of Testing Dataset

Metrics	Accuracy	STD (+/-)	Precision	Recall	F1 Score
LR	0.983	0.0055	0.98	0.98	0.98
SVM	0.982	0.0064	0.98	0.98	0.98
DT	0.994	0.016	0.99	0.99	0.99
RF	0.994	0.014	0.99	0.99	0.99

ANN	0.994	0.021	0.99	0.99	0.99

To summarize the performance of the applied models using the confusion matrix on 30 percent of the dataset samples, Random Forest demonstrated the best performance for the proposed work. Random Forest effectively classified most attack types with minimal misclassification. Out of 1,734 DoS samples, Random Forest misclassified only 589 as Normal. For Scan with 464 samples, Malicious Control with 266 samples, Malicious Operation with 241 samples, spying with 159 samples, Data Type Probing with 102 samples, and Wrong Setup with 36 samples, Random Forest achieved perfect classification with no misclassification. Additionally, Random Forest accurately predicted 69,558 samples as Normal, showcasing its superior accuracy.

In comparison, Logistic Regression and Support Vector Machine exhibited significantly lower accuracy and higher misclassification rates. Random Forest achieved better precision in classifying attacks like DoS, Scan, Malicious Control, Malicious Operation, Spying, Data type Probing and Wrong Setup compared to other models.

Figure 4. presents the confusion matrix, which shows the performance of the Random Forest model on 30% of the dataset samples. The results emphasize the Random Forest model's ability to minimize misclassification and provide reliable classification for the dataset, outperforming other techniques like LR, SVM and techniques

Predicted \ Actual	DoS	Scan	Malicious Control	Malicious Operation	Spying	Data Type Probing	Wrong Setup	Normal
DoS	1,145	0	0	0	0	0	0	589
Scan	0	464	0	0	0	0	0	0
Malicious Control	0	0	266	0	0	0	0	0
Malicious Operation	0	0	0	241	0	0	0	0
Spying	0	0	0	0	159	0	0	0
Data Type Probing	0	0	0	0	0	102	0	0
Wrong Setup	0	0	0	0	0	0	36	0
Normal	0	0	0	0	0	0	0	69,558

Figure 4. Confusion Matrix for Random Forest Model Performance on the Dataset

CONCLUSION

This ML evaluation gives an insight of that the Random Forest (RF) approach is highly effectiveness for detecting vulnerabilities in IoT network system. RF model is performed superior performance in accurately predicting vulnerabilities and attacks such as DoS, Scan, Data Probing, Malicious Control, Malicious Operation, Spying, and Wrong Setup, whereas compared to another ML models. Moreover, the RF performed well in predicting DoS and Normal dataset samples high accurately than other standard models. Therefore, this evaluation work, concluded that RF is highly suitable model for IoT systems attack and anomaly detection. This evaluation method is value add method to vulnerability prediction in the classical ML approaches, and no novel or enhanced algorithm was employed in this evaluation. Therefore, further research is needed to propose more enriched detection algorithms and discovering the overall framework design in superior requirement. Additionally, this evaluation performance was conducted using virtual environment data, and real-time data may present more challenges. A more empirical feature study focusing on real-time data and also it also necessary to address real time vulnerability issues. Further studies and implementations are needed to investigate deeper into IoT network vulnerability issues. Among all models, RF attained the highest accuracy (0.994/0.99) along with lowest F1 score variance (STD ±0.014), indicating superior and stable. Therefore, the RF as the best model and performed great in this evaluation work with an accuracy along with F1 score other than another compared model. This result may not be guaranteed in the case of another larger datasets or unpredicted dataset. Therefore, more research evaluation is required to evaluate the reliability and performance of RF under various circumstances

REFERENCE

[1] V. Meshram, K. Patil, V. Meshram, D. Hanchate, and S. D. Ramkteke, "Machine learning in agriculture domain: A state-of-art survey," *Artificial Intelligence in the Life Sciences*, vol. 1, p. 100010, Dec. 2021, doi: 10.1016/j.ailsci.2021.100010.

[2] C. Chen, Y. Liu, X. Sun, C. D. Cairano-Gilfedder, and S. Titmus, "Automobile Maintenance Prediction Using Deep Learning with GIS Data," *Procedia CIRP*, vol. 81, pp. 447–452, 2019, doi: 10.1016/j.procir.2019.03.077.

[3] R. S. Thakur, "Expense tracker management system using machine learning," *Sigma J Eng Nat Sci - Sigma Müh Fen Bil Derg*, pp. 1265–1275, 2025, doi: 10.14744/sigma.2025.00119.

[4] S. Z. El Mestari, G. Lenzini, and H. Demirci, "Preserving data privacy in machine learning systems," *Computers & Security*, vol. 137, p. 103605, Feb. 2024, doi: 10.1016/j.cose.2023.103605.

[5] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, "Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research," *Applied Sciences*, vol. 11, no. 12, p. 5713, Jun. 2021, doi: 10.3390/app11125713.

[6] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/j.iot.2022.100564.

[7] T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, vol. 13, no. 4, p. 683, Apr. 2023, doi: 10.3390/brainsci13040683.

[8] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, "Enhancing intrusion detection in IoT

networks using machine learning-based feature selection and ensemble models," *Systems Science & Control Engineering*, vol. 12, no. 1, p. 2321381, Dec. 2024, doi: 10.1080/21642583.2024.2321381.

[9] D. Sarathkumar, R. A. Raj, S. Sidthik Akbar, R. Rajesh Kanna, L. J. B. Andrews, and A. Alagappan, "IOT Based Motor Control and Line Detection for Smart Agriculture," in *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India: IEEE, Feb. 2024, pp. 1–6. doi: 10.1109/SCEECS61402.2024.10482316.

[10] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, 2023, doi: 10. 1016/j.iotcps.2022.12.003.

[11] Z. Ahmad *et al.*, "Anomaly Detection Using Deep Neural Network for IoT Architecture," *Applied Sciences*, vol. 11, no. 15, p. 7050, Jul. 2021, doi: 10.3390/app11157050.

[12] N. C. Dang, M. N. Moreno-García, and F. De La Prieta, "Sentiment Analysis Based on Deep Learning: A Comparative Study," *Electronics*, vol. 9, no. 3, p. 483, Mar. 2020, doi: 10.3390/electronics9030483.

[13] W. Jiang, "A Machine Vision Anomaly Detection System to Industry 4.0 Based on Variational Fuzzy Autoencoder," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–10, Mar. 2022, doi: 10.1155/2022/1945507.

[14] F. Ye and W. Zhao, "A Semi-Self-Supervised Intrusion Detection System for Multilevel Industrial Cyber Protection," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–11, Sep. 2022, doi: 10.1155/2022/4043309.

[15] M.-Q. Tran, M. Elsisi, K. Mahmoud, M.-K. Liu, M. Lehtonen, and M. M. F. Darwish, "Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment," *IEEE Access*, vol. 9, pp. 115429–115441, 2021, doi: 10.1109/ACCESS.2021.3105297.

[16] M. Aljabri *et al.*, "IoT Attacks Detection Using Supervised Machine Learning Techniques," *HighTech. Innov. J.*, vol. 5, no. 3, pp. 534–550, Sep. 2024, doi: 10.28991/HIJ-2024-05-03-01.

[17] H. Gupta, S. Sharma, and S. Agrawal, "Artificial Intelligence-Based Anomalies Detection Scheme for Identifying Cyber Threat on IoT-Based Transport Network," *IEEE Trans. Consumer Electron.*, vol. 70, no. 1, pp. 1716–1724, Feb. 2024, doi: 10.1109/TCE.2023.3329253.

[18] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, "A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks," *Procedia Computer Science*, vol. 210, pp. 94–103, 2022, doi: 10.1016/j.procs.2022.10.124.

[19] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/j.aej.2022.02.063.

[20] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 144–149, Jun. 2021, doi: 10.1109/MWC.001.2000428.

[21] Y. Qian, "The Future of e-Health and Wireless Technologies," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 2–3, Jun. 2021, doi: 10.1109/MWC.2021.9490593.

[22] A. Alzahrani and T. H. H. Aldhyani, "Artificial Intelligence Algorithms for Detecting and Classifying MQTT Protocol Internet of Things Attacks," *Electronics*, vol. 11, no. 22, p. 3837, Nov. 2022, doi: 10.3390/electronics11223837.

[23] R. Khilar *et al.*, "Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–10, Apr. 2022, doi: 10.1155/2022/1440538.

[24] M. Anwer, S. M. Khan, M. U. Farooq, and . Waseemullah, "Attack Detection in IoT using Machine Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, doi: 10.48084/etasr.4202.

[25] V. R. Joseph, "Optimal ratio for data splitting," *Statistical Analysis*, vol. 15, no. 4, pp. 531–538, Aug. 2022, doi: 10.1002/sam.11583.

[26] "DS2OS traffic traces." Accessed: Jan. 17, 2025. [Online]. Available: https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces

[27] L. Morán-Fernández, V. Bólon-Canedo, and A. Alonso-Betanzos, "How important is data quality? Best classifiers vs best features," *Neurocomputing*, vol. 470, pp. 365–375, Jan. 2022, doi: 10.1016/j.neucom.2021.05.107.

[28] K. Mithran and C. Gopi, "Anomaly Detection in IoT Sensor Networks using Machine Learning," in *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, Kochi, India: IEEE, Jun. 2022, pp. 1–7. doi: 10.1109/IC3SIS54991.2022.9885575.

[29] M. Hasan, Md. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[30] I. H. Sarker, "Machine Learning: Algorithms,

Real-World Applications and Research Directions," *SN COMPUT. SCI.*, vol. 2, no. 3, p. 160, May 2021, doi: 10.1007/s42979-021-00592-x.

[31] H. N. Noura, T. Chu, Z. Allal, O. Salman, and K. Chahine, "A comparative study of ensemble methods and multi-output classifiers for predictive maintenance of hydraulic systems," *Results in Engineering*, vol. 24, p. 102900, Dec. 2024, doi: 10.1016/j.rineng.2024.102900.

[32] T. Talaei Khoei and N. Kaabouch, "Machine Learning: Models, Challenges, and Research Directions," *Future Internet*, vol. 15, no. 10, p. 332, Oct. 2023, doi: 10.3390/fi15100332.

[33] Y. Xu, B. Klein, G. Li, and B. Gopaluni, "Evaluation of logistic regression and support vector machine approaches for XRF based particle sorting for a copper ore," *Minerals Engineering*, vol. 192, p. 108003, Feb. 2023, doi: 10.1016/j.mineng.2023.108003.

[34] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, p. 100163, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.

[35] Z. Sun, G. Wang, P. Li, H. Wang, M. Zhang, and X. Liang, "An improved random forest based on the classification accuracy and correlation measurement of decision trees," *Expert Systems with Applications*, vol. 237, p. 121549, Mar. 2024, doi: 10.1016/j.eswa.2023.121549.

[36] V. Shukla, A. R. Raipurkar, and M. B. Chandak, "Blockchain and ML in land registries a transformative alliance," *IJ-ICT*, vol. 13, no. 2, p. 239, Aug. 2024, doi: 10.11591/ijict.v13i2.pp239-247.

[37] M. M. Taye, "Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions," *Computers*, vol. 12, no. 5, p. 91, Apr. 2023, doi: 10.3390/computers12050091.

[38] N. Punetha and G. Jain, "Optimizing Sentiment Analysis: A Cognitive Approach with Negation Handling via Mathematical Modelling," *Cogn Comput*, vol. 16, no. 2, pp. 624–640, Mar. 2024, doi: 10.1007/s12559-023-10227-3.

[39] "Deep Learning - Day 21 - Model Evaluation and Performance Metrics," Le's Zone. Accessed: Mar. 07, 2025. [Online]. Available: https://leyao-daily.github.io/2023/05/11/Deep-Learning-Daily/

[40] S. Szeghalmy and A. Fazekas, "A Comparative Study of the Use of Stratified Cross-Validation and Distribution-Balanced Stratified Cross-Validation in Imbalanced Learning," *Sensors*, vol. 23, no. 4, p. 2333, Feb. 2023, doi: 10.3390/s23042333.