ENSEMBLE LEARNING FOR REAL-TIME ANOMALY DETECTION AND PREDICTIVE MAINTENANCE IN SMART FACTORIES

Lahcen Idouglid[1*] – Said Tkatek[1] – Khalid Elfayq[1] -- Toufik Mzili[2]

[1] Faculty of Sciences, Computer Sciences Research Laboratory, Ibn Tofail University, Kenitra, Morocco
[2]LAROSERI Lab, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco

ARTICLE INFO

***Article history*:**
Received: 13.09.2024.
Received in revised form: 11.03.2025.
Accepted: 12.03.2025.

Keywords:
Ensemble Learning
Industrial Internet of Things (IIoT)
Intrusion Detection Systems (IDS)
Smart manufacturing
XGBoost
LightGBM

DOI: https://doi.org/10.30765/er.2633

Abstract:

This paper explores the use of several ensemble learning algorithms Gradient Boosting, XGBoost, LightGBM, Bagging, AdaBoost, and Voting Classifier on the CICIoT2023 dataset within the framework of Industrial Internet of Things (IIoT) and Intrusion Detection Systems (IDS). The main goal is to improve anomaly detection and predictive maintenance in smart manufacturing environments. The models' performance was assessed using key metrics such as precision, recall, accuracy, F1 score, and ROC AUC score, in addition to evaluating their training and prediction times. Results show that Bagging and Voting Classifiers achieved the highest accuracy and ROC AUC scores, making them highly effective for complex detection tasks. However, XGBoost and LightGBM demonstrated superior computational efficiency, making them suitable for real-time systems requiring fast prediction times. The findings indicate that ensemble learning techniques can significantly improve both the accuracy and speed of anomaly detection in IIoT systems, providing a robust framework for enhancing cybersecurity and operational efficiency in smart factories.

1 Introduction

The advent of Industry 4.0 has revolutionized the manufacturing sector by introducing smart factories, which leverage the Industrial Internet of Things (IIoT) to enhance operational efficiency and decision-making [1], [2]. IIoT enables factories to connect vast networks of devices, sensors and actuators that collect, share, and analyze real-time data[3]. These innovations have provided significant advancements in areas such as real-time monitoring, predictive maintenance, and operational optimization, thereby allowing industries to reduce downtime and increase productivity [4]. A critical benefit of IIoT lies in predictive maintenance, where machine learning models analyze historical sensor data to predict equipment failures before they occur. This proactive approach prevents unexpected breakdowns, minimizes downtime, and extends the lifespan of industrial equipment [5]. Furthermore, predictive maintenance reduces maintenance costs and mitigates the risk of catastrophic failures that can disrupt production lines. Another crucial application of IIoT is real-time anomaly detection, which involves monitoring operational data streams to detect irregularities that might indicate malfunctions or quality control issues [6]. For instance, anomalies in temperature, vibration, or other metrics can signal early signs of equipment wear or inefficiencies. However, the success of such systems depends heavily on the accuracy and reliability of the underlying machine learning algorithms. Despite these advancements, traditional machine learning approaches face significant challenges when applied to the vast and heterogeneous data generated by IIoT systems. These include computational inefficiency, poor scalability, and vulnerability to overfitting, particularly when dealing with high-dimensional or imbalanced datasets [7]. Additionally, the complex nature of IIoT data, which often includes a mix of continuous and categorical features, as well as missing values, exacerbates these limitations. Ensemble learning has emerged as a promising solution to address these challenges [8]. By combining the predictions of multiple models, ensemble

* Corresponding author Lahcen Idouglid
E-mail address: lahcen.idouglid@uit.ac.ma

techniques leverage the strengths of individual algorithms to produce more accurate and stable predictions. This approach helps mitigate common issues such as overfitting or bias, making ensemble learning particularly suited for the complex environments of smart factories. Among ensemble learning methods, Gradient Boosting, Bagging, and Voting classifiers have demonstrated notable success. Gradient Boosting builds models sequentially, with each iteration correcting the errors of the previous one to minimize loss and enhance accuracy [9]. Bagging independently trains multiple models on different data subsets, reducing variance and improving generalization [10]. Voting classifiers aggregate the predictions of multiple models, producing a final prediction based on majority voting, which leverages the strengths of each contributing model [11]. While ensemble learning techniques have been widely adopted in domains such as finance, healthcare, and cybersecurity, their application to IIoT and smart manufacturing remains relatively underexplored [12]. Given the critical need for accurate, real-time decision-making in smart factories, ensemble learning presents an opportunity to optimize predictive maintenance and anomaly detection tasks.

This paper addresses these gaps by demonstrating the potential of ensemble learning techniques in tackling key challenges in IIoT applications for smart manufacturing. Specifically, it evaluates the performance of advanced ensemble methods—such as Bagging and Voting Classifiers—for predictive maintenance and anomaly detection. The study highlights how these models achieve superior accuracy, reliability, and computational efficiency, making them suitable for real-time industrial applications. The results affirm that ensemble learning not only enhances detection capabilities but also provides robust, scalable solutions for next-generation industrial systems [13]. By leveraging advanced ensemble techniques, this work contributes a comprehensive framework for improving cybersecurity, operational resilience, and efficiency in smart factories. This framework underscores the transformative potential of IIoT-based applications and positions ensemble learning as a critical tool for advancing Industry 4.0 initiatives [14]. This paper is organized as follows: Section II reviews related works on machine learning and ensemble techniques in IIoT and smart manufacturing. Section III details the methodology, including dataset description, preprocessing, algorithms, and evaluation metrics. Section IV presents the results and analysis of the ensemble algorithms applied to the CICIoT2023 dataset. Section V concludes with key findings and future research directions.

2 Related Works

The application of machine learning and ensemble techniques in IIoT and smart manufacturing systems is a growing research field, with various studies focusing on improving anomaly detection, predictive maintenance, and decision support systems. Below is an organized overview of relevant works drawn from recent literature. In 2021, Yu-Hsin Hung presented an enhanced ensemble-learning algorithm specifically designed for predictive maintenance in the semiconductor and blister packaging industries. This model integrates adaptive boosted decision trees with neural networks to improve the accuracy of predicting equipment failures and product quality degradation. The approach achieved an impressive accuracy of 99.2% in blister packaging and 97.4% in semiconductor manufacturing, highlighting its potential to significantly enhance predictive maintenance in industrial processes [15]. In 2023 Awotunde proposed an Ensemble Tree-Based Model for Intrusion Detection in IIoT networks, leveraging ensemble methods like XGBoost, Random Forest, and AdaBoost combined with chi-square feature selection. Tested on the TON_IoT datasets, the model achieved accuracies of 98.73% on the Fridge dataset and 98.83% on the Thermostat dataset, demonstrating the strength of tree-based models for cyberattack detection in IIoT environments [16]. In 2021, Shrivastav and Kumar developed an ensemble model that combines Random Forest (RF), Gradient Boosting Machine (GBM), and Deep Learning (DL) to enhance stock price prediction. When applied to a large stock market dataset, the model achieved a 99% accuracy rate, surpassing the performance of each individual model. While the study is centered on finance, the ensemble approach demonstrates its broader potential for effectively managing large, complex datasets in IIoT applications [17]. In (2024) Konatham presented a Hybrid CNN-GRU Model for Anomaly Detection in IIoT systems, focusing on edge computing environments. Their model achieved 96.41% accuracy, demonstrating the advantages of combining spatial and temporal features to improve detection of real-time cyber threats in IIoT networks [18]. In 2023 Lee developed a novel approach for Anomaly Detection Using an Ensemble of Multi-Point LSTMs. By employing LSTM networks and combining them in an ensemble model, they achieved high anomaly detection accuracy, with 95.87% accuracy on the MobiAct dataset and 97.66% accuracy on the SWaT dataset. This method highlights the strength of neural networks in processing time-series data for industrial applications [19]. In 2022, Naik conducted a comparative analysis of

machine learning algorithms for anomaly detection in IIoT environments. The study found that Random Forest consistently outperformed other algorithms across multiple datasets, achieving accuracy rates of up to 99% for detecting anomalies in IIoT systems. This research highlights the critical role of selecting the most suitable algorithms for effective anomaly detection in industrial settings [20]. Koo (2023) proposed a Double Ensemble Technique for Predicting Weight Defects in injection-molded products used in smart manufacturing. By combining bagging and boosting in a double ensemble, they achieved an accuracy of 97.98%, demonstrating improvements in defect prediction and product quality maintenance in smart factories[21]. In 2022 Hazman introduced IDS-SIoEL, an Intrusion Detection Framework for securing IoT-based smart environments. This framework leverages ensemble methods like AdaBoost and advanced feature selection techniques to achieve near-perfect detection rates, with 99.99% accuracy on the BoT-IoT dataset.

The study emphasizes the role of ensemble learning in improving security in IoT systems[22]. Rodriguez and colleagues developed a prediction model for smart aquaponic systems using a combination of Bagging and Boosting Ensemble Techniques. The model was integrated into an autonomous IIoT-based aquaponic management system to optimize water quality for plants and fish. Key parameters such as dissolved oxygen, pH, and water temperature were monitored and processed using machine learning. The study showed that the bagging-based model achieved a test accuracy of 94.09%, while the boosting-based model improved this to 95.23%, illustrating the effectiveness of ensemble learning in precision agriculture[10]. Kotsiopoulos (2020) explored the application of Machine Learning (ML) and Deep Learning (DL) in smart manufacturing and smart grids within the context of Industry 4.0. The study proposes a comprehensive Industrial Artificial Intelligence (IAI) architecture, integrating various ML and DL models, including Random Forest, SVM, CNN, and RNN, to optimize predictive maintenance, fault detection, and energy efficiency in industrial environments. The authors highlight the high performance of DL models in handling complex data but also note the challenges posed by computational costs and data requirements[23]. Maha Al-Sharif and Anas Bushnag, (2024) proposed an ensemble learning-based intrusion detection system (IDS) to enhance cloud security. Using the CICIDS2017 dataset, they evaluated techniques like bagging, AdaBoost, LPBoost, and RUSBoost. The study found that Ensemble RUSBoost achieved the highest accuracy of 99.821%, demonstrating superior threat detection compared to traditional models [24]. El Hajla (2024) proposed a hybrid ensemble approach for intrusion detection in IoT networks, combining methods like AdaBoost, random forest, and SVM to improve threat detection accuracy and reduce false positives. Using the CICIDS2017 dataset, their study demonstrates the effectiveness of ensemble learning in enhancing IDS resilience for IoT environments [25]. The paper [26] presents the Discrete Rat Swarm Optimizer (DRSO) as a new method for solving the Quadratic Assignment Problem (QAP), an NP-hard problem.

The authors introduce a mapping strategy to convert real values to discrete values and redefine operators for combinatorial problems. They also incorporate 2-opt and 3-opt local search heuristics to improve solution quality. Simulations using the QAPLIB test library and statistical analysis show that DRSO outperforms other algorithms in terms of solution quality, convergence speed, and deviation from best-known values, proving it to be an efficient approach for solving QAP. The last paper [27] introduces a novel hybrid approach combining Genetic Algorithms (GA) and Penguin Search Optimization (PSeOA) to solve the Flow Shop Scheduling Problem (FSSP). The GA employs natural selection mechanisms such as selection, crossover, and mutation, while PSeOA mimics penguin foraging behavior to enhance exploration. The hybrid method integrates GA's genetic diversity with PSeOA's fast convergence, with modifications tailored for FSSP. Experimental results show that the hybrid approach outperforms pure GA, PSeOA, and other metaheuristic algorithms in terms of solution quality and efficiency. The table summarizes recent works on applying ensemble learning in IIoT and smart manufacturing. These studies focus on predictive maintenance, anomaly detection, and decision support, using various machine learning and deep learning algorithms, from tree-based models like Random Forest and XGBoost to advanced hybrid models like CNNs and LSTMs, to improve accuracy and reliability in complex industrial environments.

Table 1. Summary of Related Works.

Authors	Year	Methods	Algorithms	Accuracy/Results
Yu-Hsin Hung	2021	Predictive Maintenance	Boosted Decision Trees, Neural Networks	97.4% (Semiconductor), 99.2% (Blister Packaging)
Awotunde et al.	2023	Intrusion Detection in IIoT	XGBoost, Random Forest, AdaBoost	98.73% (Fridge), 98.83% (Thermostat)
Shrivastav and Kumar	2021	Stock Price Prediction	Gradient Boosting, Random Forest, Deep Learning	99% (Stock Market Prediction)
Konatham et al.	2024	Anomaly Detection in IIoT (Edge Computing)	Hybrid CNN-GRU	96.41%
Lee et al.	2023	Anomaly Detection in Time-Series	Multi-Point LSTM Ensemble	95.87% (MobiAct), 97.66% (SWaT)
Naik et al.	2022	Comparative Analysis for Anomaly Detection	Random Forest, LightGBM, Decision Trees	Up to 99% (Anomaly Detection in IIoT)
Koo et al.	2023	Weight Defect Prediction in Manufacturing	Double Ensemble (Bagging and Boosting)	97.98%
Hazman et al.	2022	Intrusion Detection for IoT Networks	AdaBoost, Feature Selection	99.99% (BoT-IoT)
Kotsiopoulos et al.	2020	Smart Manufacturing & Smart Grids	Random Forest, SVM, CNN, RNN	High Performance in Smart Grid Applications
Rodriguez et al.	2023	Decision Support in Aquaponic Systems	Bagging and Boosting Ensemble Techniques	96.93% (Bagging), 95.23% (Boosting)
Maha Al-Sharif, Anas Bushnag	2024	Ensemble Learning-based Intrusion Detection System (IDS)	Bagging, AdaBoost, LPBoost, RUSBoost	Ensemble RUSBoost achieved the highest performance with 99.821% accuracy
El Hajla	2024	Hybrid Ensemble Learning Approach for Intrusion Detection	AdaBoost, Random Forest, Support Vector Machines (SVM)	Improved detection accuracy and reduced false positive rates using CICIDS2017 dataset
Mzili et al.	2023	Discrete Rat Swarm Optimizer (DRSO)	Rat Swarm Optimization (QAP)	The DRSO algorithm outperforms other algorithms in solving the QAP, demonstrating superior solution quality, faster convergence, and lower deviation from the best-known values.
Mzili et al.	2024	Hybrid Genetic Algorithm and Penguin Search Optimization (PSeOA)	Flow Shop Scheduling Problem (FSSP)	The hybrid approach outperforms pure GA, PSeOA, and other metaheuristics in terms of solution quality and efficiency in solving the FSSP.

These studies collectively demonstrate the growing importance of ensemble learning in enhancing the performance of machine learning models across diverse industrial applications. By integrating multiple

algorithms, ensemble methods consistently deliver superior accuracy and robustness, making them essential for addressing the challenges posed by large-scale, heterogeneous IIoT data. As the field continues to evolve, these advancements in predictive analytics, anomaly detection, and decision support systems will play a critical role in driving the next generation of smart manufacturing and industrial automation.

3 Methodology

This research aims to advance the state of predictive maintenance and anomaly detection in smart factories by leveraging the strengths of ensemble learning algorithms applied to IIoT data. By utilizing the CICIoT2023 dataset, which is specifically designed to represent the complexity and scale of IIoT network traffic and operational data, this study not only demonstrates the efficacy of ensemble methods in industrial environments but also provides a comprehensive analysis of their performance across various metrics. The methodology is carefully designed to address the challenges posed by the vast and heterogeneous nature of IIoT data, employing state-of-the-art preprocessing techniques, hyperparameter optimization, and robust validation strategies to ensure the reliability and applicability of the results in real-world smart manufacturing contexts. This approach highlights the potential of ensemble learning to enhance both the accuracy and speed of predictive models, offering a scalable and adaptive solution for improving the cybersecurity and operational efficiency of next-generation industrial systems.

3.1 Dataset Description

The CICIoT2023 dataset [28], created by the Canadian Institute for Cybersecurity, is one of the most recent and detailed datasets available for IIoT applications. It includes a wide range of features extracted from IIoT devices, covering both normal and malicious activities. This dataset is particularly suited for anomaly detection, as it encompasses real-world scenarios of both normal operations and various attack vectors. The dataset was preprocessed to remove any missing values, normalize the features, and balance the class distributions to ensure a robust training process for the models [29]. The URL to access this dataset, is: https://www.unb.ca/cic/datasets/ In addition to its comprehensive feature set, the CICIoT2023 dataset offers detailed labels for each instance, making it highly suitable for supervised learning tasks. Its attack scenarios include Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) attacks, and data injection, providing a broad spectrum of challenges for machine learning models. Furthermore, the dataset's focus on IIoT-specific characteristics, such as sensor data patterns and communication protocols, allows researchers to develop and test models under conditions closely resembling real-world IIoT environments. This specificity makes CICIoT2023 a valuable resource for advancing cybersecurity and operational efficiency in smart manufacturing systems.

3.2 Principal Steps

The methodology involved several key steps, outlined as follows:

3.2.1 Data Preprocessing

- *Feature Selection:* Initial feature selection was conducted to reduce the dimensionality of the dataset and retain the most relevant features for the predictive tasks. Techniques such as recursive feature elimination and correlation analysis were employed to identify the most impactful features [30].
- *Data Normalization:* To ensure that all features contribute equally to the learning process, the data was normalized using MinMax scaling, bringing all features into the range [0, 1] [31].
- *Train-Test Split:* The dataset was partitioned into training (80%) and testing (20%) sets using stratified sampling to preserve the original class distribution.

3.2.2 Evaluation Metrics

The models were assessed using a range of performance metrics, including ROC AUC score, recall, precision, F1-score, and accuracy. Additionally, the confusion matrix was employed to gain deeper insights into the classification performance, specifically examining the rates of true positives, true negatives, false positives, and false negatives [32].

3.2.3 Training and Testing

Each model was trained on the CICIoT2023 dataset using stratified k-fold cross-validation to ensure strong generalization to new data. To optimize performance, a grid search method was employed for hyperparameter tuning, identifying the most effective parameter combinations for each algorithm [13].

3.2.4 Performance Comparison

After training and validation, the models' performance was compared using the evaluation metrics, with particular focus on their ability to detect anomalies and failures while minimizing false positives and false negatives. The results were compiled into a table that presented each algorithm's confusion matrix, recall, precision, F1 score, accuracy, and computational efficiency, measured in terms of training and testing time [33].

3.3 Algorithms and Implementation

The algorithms were implemented using Python and popular machine learning libraries such as scikit-learn, XGBoost, and LightGBM [34]. The steps were as follows:

- *Gradient Boosting:* Implemented using scikit-learn's GradientBoostingClassifier, the model was fine-tuned to optimize for both speed and accuracy, with key hyperparameters like learning rate, number of estimators, and maximum depth being adjusted [35].
- *XGBoost:* Using the XGBClassifier from the `xgboost` library, hyperparameter tuning focused on tree depth, learning rate, and regularization terms to control overfitting and improve generalization [36].
- *LightGBM:* Implemented using LGBMClassifier from the `lightgbm` library, this algorithm was optimized for speed and memory usage, with leaf-wise growth strategies being preferred to depth-wise [37].
- *Bagging:* Scikit-learn's BaggingClassifier was used with a variety of base estimators, primarily decision trees, to create an ensemble that averaged out the noise and variance from individual models [38].
- *AdaBoost:* The AdaBoostClassifier from scikit-learn was utilized, with weak learners being adjusted to improve performance on hard-to-classify instances in the dataset [39].
- *Voting Classifier:* The ensemble of classifiers was combined using a hard voting mechanism where each classifier's predictions were weighted equally.

3.4 Methodology Flowchart Representation

The methodology follows a clear and structured process that begins with dataset preparation and ends with model evaluation, ensuring a thorough and effective approach to predictive maintenance and anomaly detection. This linear approach ensures that each step contributes to building a highly accurate and reliable predictive model for IIoT systems.

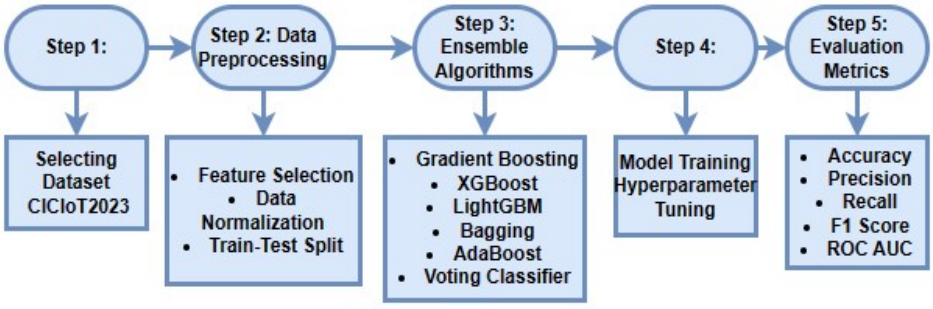

Figure 1. Linear Flowchart Representation of Methodology.

This graphical flowchart effectively organizes the entire process from dataset acquisition to model evaluation, making the methodology clear and linear.

- *Step 1:* Dataset - CICIoT2023
  The foundation of the analysis is the CICIoT2023 dataset, providing the necessary data for model training and testing.
- *Step 2:* Data Preprocessing
  Key actions include feature selection, data normalization, and train-test splitting, which prepare the data for optimal model performance.
- *Step 3:* Ensemble Algorithms
  Multiple ensemble learning techniques (Gradient Boosting, XGBoost, LightGBM, Bagging, AdaBoost, and Voting Classifier) are implemented to enhance predictive accuracy and robustness.
- *Step 4:* Model Training & Hyperparameter Tuning
  Models are trained and fine-tuned using hyperparameter optimization to achieve the best performance on the preprocessed dataset.
- *Step 5:* Evaluation Metrics
  The effectiveness of the models is assessed using a range of evaluation metrics: precision, recall (sensitivity), F1 score, ROC AUC, and accuracy. These metrics are crucial for evaluating the performance of anomaly detection systems, as they provide a comprehensive understanding of how well the models distinguish between normal and anomalous instances in IIoT environments. Specifically, they help assess the trade-off between correctly identifying anomalies and minimizing false alarms, which is critical in predictive maintenance and anomaly detection.
- Accuracy (ACC): Measures the proportion of correct predictions (true positives and true negatives). It can be misleading with imbalanced data, as it may not reflect effective anomaly detection. The ACC metric is calculated in Eq. (1):

$$\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{1}$$

- Precision: Indicates the proportion of predicted anomalies that are true anomalies. High precision minimizes false positives, avoiding unnecessary alerts. The metric is calculated using Eq. (2):

$$\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}, \tag{2}$$

- Recall (Sensitivity): Measures the proportion of actual anomalies correctly identified by the model. High recall ensures most anomalies are detected, important for predictive maintenance.

$$\text{True Positive / (False Negative + True Positive)} \tag{3}$$

- F1 Score: The harmonic mean of precision and recall, balancing both metrics. It's useful in imbalanced datasets, ensuring the model performs well in both detection and accuracy.

$$\text{2 * ((Precision * Sensitivity) / (Precision + Sensitivity))} \tag{4}$$

- ROC AUC: Reflects the model's ability to differentiate between positive and negative classes. A higher AUC indicates better discrimination, especially in imbalanced datasets.

Together, these metrics provide a well-rounded evaluation framework to determine the most suitable model for anomaly detection and predictive maintenance in IIoT systems, ensuring that the model performs optimally in identifying anomalies while minimizing false alarms.

4 Results and Discussion

In this section, we evaluate the performance of six ensemble learning algorithms (Gradient Boosting, XGBoost, LightGBM, Bagging, AdaBoost, and Voting Classifier) applied to the CICIoT2023 dataset. The performance of the models was evaluated using key metrics, including accuracy, precision, recall, F1-score, and ROC AUC. As shown in Table 2, Bagging achieved the highest accuracy (99.750%), while XGBoost demonstrated the fastest prediction time (7.88 ms), making it ideal for real-time anomaly detection.

4.1 Model Evaluation and Results

Table 2 summarizes the performance of the ensemble learning models applied to the CICIoT2023 dataset. Bagging achieved the highest accuracy of 99.750%, indicating its effectiveness in generalizing to unseen data. Meanwhile, XGBoost and LightGBM demonstrated competitive accuracies of 99.633% and 99.676%, respectively, with significantly faster training times, making them suitable for real-time applications.
Accuracy: Bagging achieved the highest accuracy at 99.750%, which suggests that this model is highly effective at distinguishing between normal and anomalous instances. This high accuracy indicates that Bagging is a strong candidate for applications where minimizing false negatives is critical, such as anomaly detection in IIoT systems.
Precision: Bagging also exhibited excellent precision (99.754%), indicating that it makes very few false positive predictions. This is crucial in IIoT applications where false alarms could lead to unnecessary interventions and higher operational costs.
Recall: With a recall of 99.750%, Bagging excels in correctly identifying anomalies. High recall is essential for ensuring that as many anomalies as possible are detected, particularly in predictive maintenance tasks where undetected issues can lead to system failures.
F1 Score: The 99.752% F1 score for Bagging indicates a well-balanced model in terms of both precision and recall. This makes it ideal for real-world applications where both false positives and false negatives need to be minimized.
ROC AUC: The ROC AUC score for Bagging was 99.972%, reflecting its outstanding ability to discriminate between normal and anomalous instances. A high AUC is particularly valuable when dealing with imbalanced datasets, as it shows the model's robustness across various decision thresholds.
Training Time: Although Bagging achieved the best performance, it required 56,044.94 seconds to train, which is significantly longer than models like XGBoost and LightGBM. This highlights a trade-off between accuracy and computational efficiency. While Bagging's performance is superior, its long training time may be a limitation in real-time applications that require frequent model updates.
Prediction Time: Bagging's prediction time was 79.04 milliseconds, which is slower compared to models like XGBoost (7.88 milliseconds) and LightGBM (29.24 milliseconds). This further emphasizes the trade-off between the higher accuracy of Bagging and its slower operational speed.

Table 2. Performance Comparison of Machine Learning Models for Intrusion Detection.

Algorithm	Accuracy	Precision	Recall	F1 Score	ROC AUC Score	Training Time (s)	Prediction Time (ms)
Gradient Boosting	99.655%	99.659%	99.655%	99.657%	99.959%	17113.25	20.48
XGBoost	99.633%	99.648%	99.633%	99.639%	99.946%	5540.97	7.88
LightGBM	99.676%	99.685%	99.676%	99.679%	99.956%	4069.92	29.24
Bagging Classifier	99.750%	99.754%	99.750%	99.752%	99.972%	56044.94	79.04
AdaBoost	99.605%	99.615%	99.605%	99.609%	99.948%	6277.16	78.60
Voting Classifier	99.716%	99.719%	99.716%	99.717%	99.971%	32072.37	193.59

4.1.1 Accuracy

The accuracy of the ensemble models is illustrated in Figure 2. Bagging emerges as the top performer, achieving an accuracy of 99.750%. This is closely followed by the Voting Classifier, which also demonstrates strong performance. These results highlight the potential of ensemble methods to improve predictive maintenance in IIoT systems.

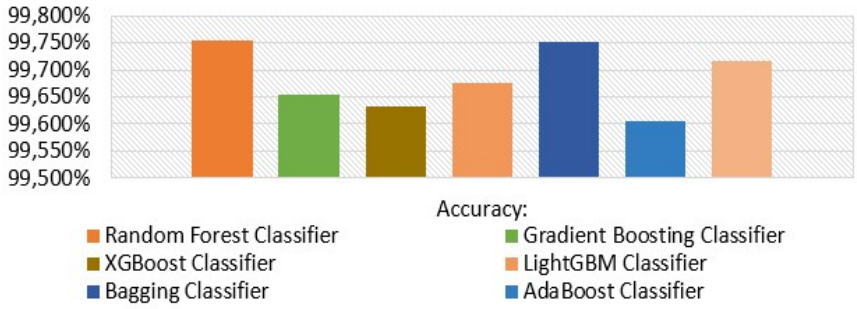

Figure 2. Comparison of Accuracy for Ensemble Learning Algorithms on the CICIoT2023 Dataset.

4.1.2 Precision and Recall

Figure 3 compares the precision and recall metrics for the evaluated models. Bagging and Voting Classifiers consistently exhibit high precision and recall values, underscoring their ability to minimize false positives and false negatives effectively. This makes these models suitable for high-stakes environments where accuracy and reliability are paramount

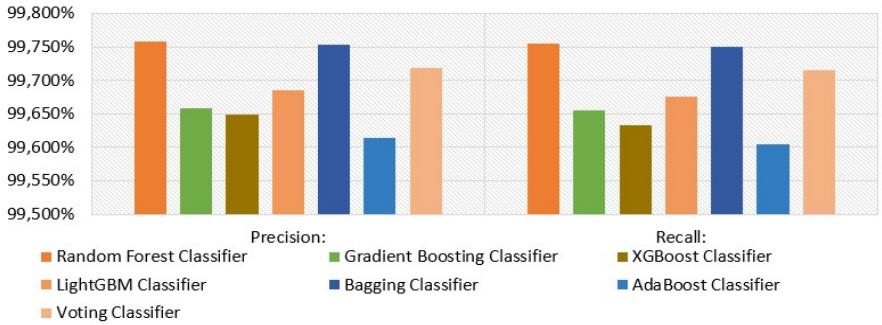

Figure 3. Comparison of Precision and Recall for Ensemble Learning Algorithms on the CICIoT2023 Dataset.

- *Bagging Classifier:* High precision and recall suggest that this model can reliably predict true positives (correctly classified events) with minimal false positives or negatives. This makes it a strong candidate for high-stakes environments such as anomaly detection in IIoT.
- *Voting Classifier:* Similar to Bagging, the Voting Classifier effectively combines the predictions of multiple models to maintain high precision and recall.

4.1.3 F1 Score

As shown in Figure 4, the F1 Score of the models reflects their balanced precision and recall. Bagging leads with an F1 Score of 99.752%, while LightGBM and XGBoost follow closely. These results emphasize the reliability of ensemble methods in maintaining high predictive performance.

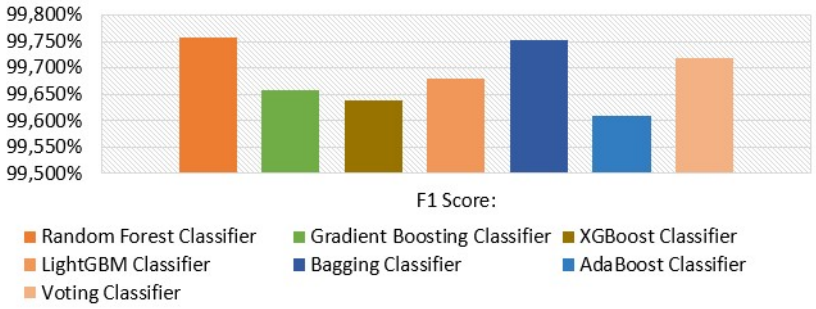

Figure 4. Comparison of F1 Score for Ensemble Learning Algorithms on the CICIoT2023 Dataset.

4.1.4 ROC AUC

The ROC AUC scores of the models are depicted in Figure 5. Bagging and Voting Classifiers achieve near-perfect scores of 99.972% and 99.971%, respectively, indicating their exceptional capability to distinguish between normal and anomalous instances. This highlights their robustness for anomaly detection in IIoT systems.

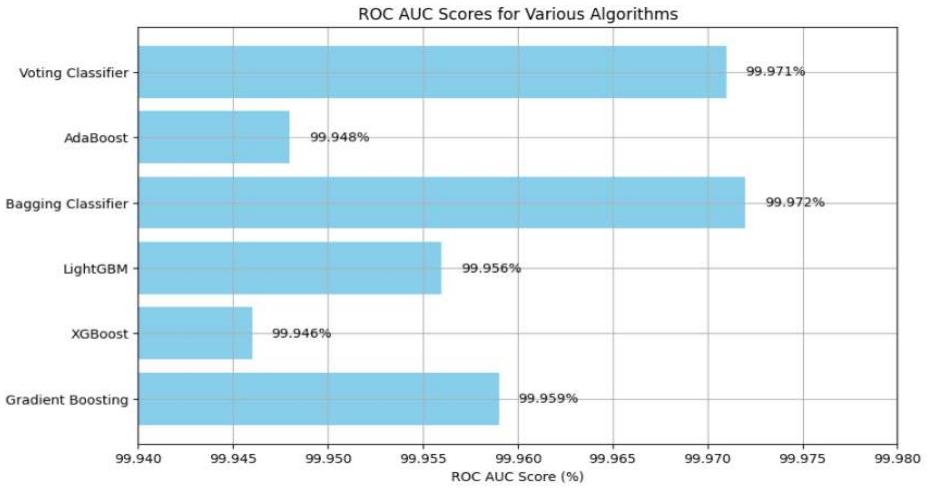

Figure 5. Comparison of ROC AUC for Ensemble Learning Algorithms on the CICIoT2023 Dataset.

4.1.5 Training and Prediction Times

Bagging Classifier required the longest training time (56044.94 seconds) due to its nature of training multiple decision trees on bootstrapped samples. In contrast, LightGBM and XGBoost demonstrated significantly faster training times of 4069.92 seconds and 5540.97 seconds, respectively, striking a balance between accuracy and computational efficiency, which makes them suitable for real-time systems. Additionally, XGBoost exhibited the fastest prediction time at 7.88 milliseconds, followed by Gradient Boosting at 20.48 milliseconds, further solidifying XGBoost's suitability for real-time anomaly detection and predictive maintenance applications.
Figure 6 shows the training and prediction times for the ensemble models. While Bagging achieves the highest accuracy, it has the longest training time, making it less suitable for real-time applications. Conversely, XGBoost exhibits the fastest prediction time of 7.88 milliseconds, offering a practical balance between computational efficiency and predictive performance.

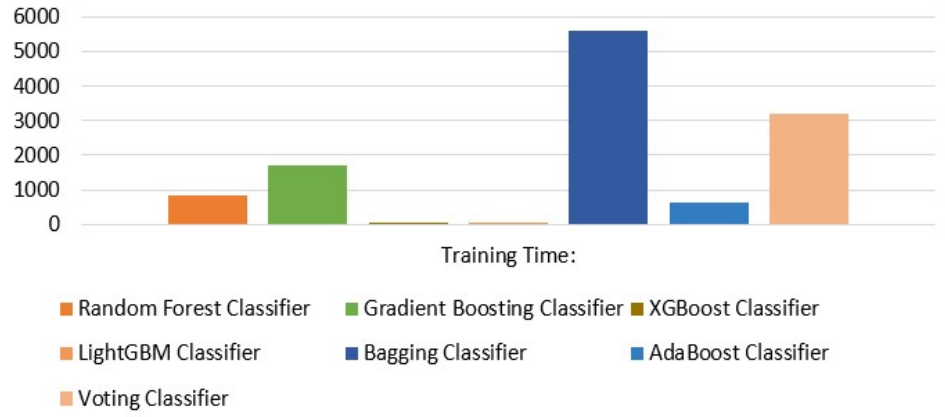

Figure 6. Comparison of Training and Prediction Times for Ensemble Learning Algorithms on the CICIoT2023 Dataset.

The performance of ensemble learning models in IIoT environments is determined not just by their accuracy but also by their computational efficiency. XGBoost stands out for its balance of 99.633% accuracy and fast prediction time of 7.88 milliseconds, making it ideal for real-time anomaly detection. LightGBM, with 99.676% accuracy and a short training time of 4069.92 seconds, excels in systems requiring quick updates while maintaining high performance. However, Bagging and Voting Classifiers offer superior accuracy but at the cost of extended training and prediction times, limiting their use in dynamic, real-time environments.
Selecting the right algorithm depends on application needs. XGBoost is optimal for real-time monitoring in IIoT networks due to its quick prediction and strong accuracy. For highly sensitive systems requiring maximum accuracy, Bagging Classifier and Voting Classifier are recommended, despite their longer computational times. These models are suitable for high-stakes applications, such as anomaly detection in critical infrastructures, where detection accuracy outweighs speed. LightGBM is an excellent choice for large-scale, dynamic environments where frequent model retraining is necessary, striking a balance between speed and predictive performance. Ensemble learning techniques, when applied to IIoT and IDS applications, enhance both security and operational efficiency. XGBoost and LightGBM excel in fast decision-making and model retraining, making them ideal for real-time and adaptive systems. Meanwhile, Bagging and Voting Classifiers provide unparalleled accuracy, best suited for high-stakes environments where precision is critical.

These algorithms collectively offer a flexible range of options, catering to various IIoT and IDS applications, from real-time intrusion detection to predictive maintenance in smart factories, ensuring improved detection and response capabilities. To further assess the performance of the ensemble learning models, we compare them with simpler baseline models, such as Decision Tree and Logistic Regression. These models serve as a reference to highlight the advantages of using more complex ensemble methods. Decision Tree is a straightforward model that builds a tree-like structure to make decisions based on input features. While it is easy to interpret, it tends to overfit and lacks the generalization power needed for complex anomaly detection tasks, especially when the dataset is imbalanced. Logistic Regression is a linear model that predicts the probability of an instance belonging to a specific class. It is computationally efficient but often struggles with complex, nonlinear relationships in the data, such as those found in IIoT environments. In comparison, ensemble methods like Bagging, XGBoost, and LightGBM consistently outperform these simpler models. These methods leverage multiple base learners, improving generalization and robustness by combining the strengths of various models. For example, while Decision Trees may suffer from overfitting, Bagging reduces this risk by averaging multiple decision trees trained on different data subsets. Similarly, XGBoost and LightGBM improve both accuracy and computational efficiency, especially in large-scale, imbalanced datasets, making them more suitable for real-time anomaly detection in IIoT systems.

5 Conclusion

This study demonstrates the significant potential of ensemble learning algorithms in improving predictive maintenance and anomaly detection for IIoT and Intrusion Detection Systems (IDS). Among the models tested,

Bagging and Voting Classifiers achieved the highest accuracy, making them well-suited for complex detection tasks where precision is critical. However, their high computational cost limits their applicability in real-time systems. In contrast, XGBoost and LightGBM strike an ideal balance between accuracy and computational efficiency, making them more suitable for real-time applications such as continuous monitoring in smart factories.The findings highlight the importance of selecting the right model based on the trade-off between performance and operational efficiency. While Bagging excels in accuracy, models like XGBoost and LightGBM provide faster processing times, which are crucial for dynamic IIoT environments where real-time decision-making is essential. This research advances the field by demonstrating how ensemble methods can be adapted to meet the demands of both high accuracy and speed, offering a robust solution for IIoT applications. Future work should focus on integrating ensemble learning techniques with deep learning models, potentially creating hybrid models that can further enhance performance by capturing both spatial and temporal data patterns in IIoT systems. Additionally, the development of lightweight models optimized for edge computing could help improve real-time decision-making by reducing the reliance on centralized servers, making anomaly detection more efficient in remote or resource-constrained environments. While this study relies on the CICIoT2023 dataset, future research should validate these models across more diverse datasets to assess their generalizability. Exploring unsupervised learning methods would also be beneficial for handling limited labeled data, which is common in real-world IIoT environments. Overall, this work contributes to enhancing the security and operational efficiency of IIoT systems, laying the groundwork for resilient, intelligent smart manufacturing systems.

References

[1] P. Zheng *et al.*, “Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives,” *Front. Mech. Eng.*, vol. 13, no. 2, pp. 137–150, Jun. 2018, doi: 10.1007/s11465-018-0499-5.

[2] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, “A NOVEL ANOMALY DETECTION MODEL FOR THE INDUSTRIAL INTERNET OF THINGS USING MACHINE LEARNING TECHNIQUES,” no. 1, 2024, doi: doi: 10.32620/reks.2024.1.12.

[3] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, “Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience,” *IJECE*, vol. 14, no. 3, p. 3512, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3512-3521.

[4] O. Peter, A. Pradhan, and C. Mbohwa, “Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies,” *Procedia Computer Science*, vol. 217, pp. 856–865, 2023, doi: 10.1016/j.procs.2022.12.282.

[5] A. M. Eid, A. B. Nassif, B. Soudan, and M. N. Injadat, “IIoT Network Intrusion Detection Using Machine Learning,” in *2023 6th International Conference on Intelligent Robotics and Control Engineering (IRCE)*, Jilin, China: IEEE, Aug. 2023, pp. 196–201. doi: 10.1109/IRCE59430.2023.10255088.

[6] A. S. Rajesh, M. S. Prabhuswamy, and S. Krishnasamy, “Smart Manufacturing through Machine Learning: A Review, Perspective, and Future Directions to the Machining Industry,” *Journal of Engineering*, vol. 2022, pp. 1–6, Aug. 2022, doi: 10.1155/2022/9735862.

[7] M. A. Shajahan, C. Roberts, A. K. Sandu, and N. Richardson, “Real-time Multimedia Analytics for IoT Applications: Leveraging Machine Learning for Insights,” *Eng. int. (Dhaka)*, vol. 12, no. 1, pp. 29–50, Feb. 2024, doi: 10.18034/ei.v12i1.713.

[8] M. S. Farooq *et al.*, “A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry,” *Sensors*, vol. 23, no. 21, p. 8958, Nov. 2023, doi: 10.3390/s23218958.

[9] M. Saied, S. Guirguis, and M. Madbouly, “A Comparative Study of Using Boosting-Based Machine Learning Algorithms for IoT Network Intrusion Detection,” *Int J Comput Intell Syst*, vol. 16, no. 1, p. 177, Nov. 2023, doi: 10.1007/s44196-023-00355-x.

[10] R. E. Rodriguez, J. T. De Castro, E. B. Sansolis, B. D. Gerardo, and Y.-C. Byun, “Prediction Model based on Bagging and Boosting Ensemble Technique for Decision Support System of Autonomous Smart IIoT Smart Aquaponic System,” *J. Phys.: Conf. Ser.*, vol. 2559, no. 1, p. 012010, Aug. 2023, doi: 10.1088/1742-6596/2559/1/012010.

[11] M. H. Ho *et al.*, "Ensemble Learning for Multi-Label Classification with Unbalanced Classes: A Case Study of a Curing Oven in Glass Wool Production," *Mathematics*, vol. 11, no. 22, p. 4602, Nov. 2023, doi: 10.3390/math11224602.
[12] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 192–204, 2023, doi: 10.1016/j.iotcps.2023.04.006.
[13] P. V, I. Sumaiya Thaseen, T. Reddy Gadekallu, M. K. Aboudaif, and E. Abouel Nasr, "Robust Attack Detection Approach for IIoT Using Ensemble Classifier," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2457–2470, 2021, doi: 10.32604/cmc.2021.013852.
[14] S. O. Alhuqayl, A. T. Alenazi, H. A. Alabduljabbar, and M. A. Haq, "Improving Predictive Maintenance in Industrial Environments via IIoT and Machine Learning," *IJACSA*, vol. 15, no. 4, 2024, doi: 10.14569/IJACSA.2024.0150464.
[15] Y.-H. Hung, "Improved Ensemble-Learning Algorithm for Predictive Maintenance in the Manufacturing Process," *Applied Sciences*, vol. 11, no. 15, p. 6832, Jul. 2021, doi: 10.3390/app11156832.
[16] J. B. Awotunde *et al.*, "An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks," *Applied Sciences*, vol. 13, no. 4, p. 2479, Feb. 2023, doi: 10.3390/app13042479.
[17] L. K. Shrivastav and R. Kumar, "An Ensemble of Random Forest Gradient Boosting Machine and Deep Learning Methods for Stock Price Prediction:," *Journal of Information Technology Research*, vol. 15, no. 1, pp. 1–19, Nov. 2021, doi: 10.4018/JITR.2022010102.
[18] B. Konatham, T. Simra, F. Amsaad, M. I. Ibrahem, and N. Z. Jhanjhi, "A Secure Hybrid Deep Learning Technique for Anomaly Detection in IIoT Edge Computing," Jan. 26, 2024. doi: 10.36227/techrxiv.170630909.96680286/v1.
[19] G. Lee, Y. Yoon, and K. Lee, "Anomaly Detection Using an Ensemble of Multi-Point LSTMs," *Entropy*, vol. 25, no. 11, p. 1480, Oct. 2023, doi: 10.3390/e25111480.
[20] Bhupal Naik D. S., V. Dondeti, and S. Balakrishna, "Comparative Analysis of Machine Learning-Based Algorithms for Detection of Anomalies in IIoT:," *International Journal of Information Retrieval Research*, vol. 12, no. 1, pp. 1–55, May 2022, doi: 10.4018/IJIRR.298647.
[21] K. Koo, K. Choi, and D. Yoo, "Double Ensemble Technique for Improving the Weight Defect Prediction of Injection Molding in Smart Factories," *IEEE Access*, vol. 11, pp. 113605–113622, 2023, doi: 10.1109/ACCESS.2023.3324192.
[22] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Comput*, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.
[23] T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, and D. Tzovaras, "Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm," *Computer Science Review*, vol. 40, p. 100341, May 2021, doi: 10.1016/j.cosrev.2020.100341.
[24] M. Al-Sharif and A. Bushnag, "Enhancing cloud security: A study on ensemble learning-based intrusion detection systems," *IET Communications*, p. cmu2.12801, Jul. 2024, doi: 10.1049/cmu2.12801.
[25] S. El Hajla, E. M. Ennaji, Y. Maleh, and S. Mounir, "Enhancing IoT network defense: advanced intrusion detection via ensemble learning techniques," *IJEECS*, vol. 35, no. 3, p. 2010, Sep. 2024, doi: 10.11591/ijeecs.v35.i3.pp2010-2020.
[26] T. Mzili, I. Mzili, M. E. Riffi, D. Pamucar, V. Simic, and M. Kurdi, "A NOVEL DISCRETE RAT SWARM OPTIMIZATION ALGORITHM FOR THE QUADRATIC ASSIGNMENT PROBLEM," *FU Mech Eng*, vol. 21, no. 3, p. 529, Oct. 2023, doi: 10.22190/FUME230602024M.
[27] T. Mzili *et al.*, "HYBRID GENETIC AND PENGUIN SEARCH OPTIMIZATION ALGORITHM (GA-PSEOA) FOR EFFICIENT FLOW SHOP SCHEDULING SOLUTIONS," *FU Mech Eng*, vol. 22, no. 1, p. 077, Apr. 2024, doi: 10.22190/FUME230615028M.
[28] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023, doi: 10.3390/s23135941.

[29] A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, "Comparative study of ML models for IIoT intrusion detection: impact of data preprocessing and balancing," *Neural Comput & Applic*, vol. 36, no. 13, pp. 6955–6972, May 2024, doi: 10.1007/s00521-024-09439-x.
[30] P. Nimbalkar and D. Kshirsagar, "Feature selection for intrusion detection system in Internet-of-Things (IoT)," *ICT Express*, vol. 7, no. 2, pp. 177–181, Jun. 2021, doi: 10.1016/j.icte.2021.04.012.
[31] S. G. K. Patro and K. K. Sahu, "Normalization: A Preprocessing Stage," *International Advanced Research Journal in Science, Engineering and Technology*, pp. 20–22, Mar. 2015, doi: 10.17148/IARJSET.2015.2305.
[32] Ž. Đ. Vujovic, "Classification Model Evaluation Metrics," *IJACSA*, vol. 12, no. 6, 2021, doi: 10.14569/IJACSA.2021.0120670.
[33] D. Powers, "Evaluation: From Precision, Recall and F-Factor to ROC, Informedness, Markedness & Correlation".
[34] Z. Benamor, Z. A. Seghir, M. Djezzar, and M. Hemam, "A Comparative Study of Machine Learning Algorithms for Intrusion Detection in IoT Networks," *RIA*, vol. 37, no. 3, pp. 567–576, Jun. 2023, doi: 10.18280/ria.370305.
[35] J. H. Friedman, "Greedy function approximation: A gradient boosting machine.," *Ann. Statist.*, vol. 29, no. 5, Oct. 2001, doi: 10.1214/aos/1013203451.
[36] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco California USA: ACM, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.
[37] G. Ke *et al.*, "LightGBM: A Highly Efficient Gradient Boosting Decision Tree".
[38] L. Breiman, "Bagging predictors," *Mach Learn*, vol. 24, no. 2, pp. 123–140, Aug. 1996, doi: 10.1007/BF00058655.
[39] Y. Freund and R. E. Schapire, "A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting," *Journal of Computer and System Sciences*, vol. 55, no. 1, pp. 119–139, Aug. 1997, doi: 10.1006/jcss.1997.1504.