International Journal of Computational Science and Engineering Research
ISSN: 3107 -8605 (Online) , http://www.ijcser.com/
Regular Issue , Vol. 2, Issue. 4 (October – December), 2025 , Pages: 55 - 61
Received: 28 May 2025 ; *Accepted:* 28 November 2025 ; *Published:* 27 December 2025
https://doi.org/10.63328/IJCSER-V2RI4P11
Original Paper : Applied Research – Compare and Contrast Research Paper

Securing Internet of Vehicles (IoV) : Robust Machine Learning Models

S Sunil Kumar [1] , G Lokesh [2]

[1, 2] Department of Computer Science and Engineering , Vemu Institute of Technology, Andhra Pradesh-517112,India;
sunilkumar473@gmail.com , lokeshgvemu@gmail.com

** Corresponding Author : S Sunil Kumar; lokeshgvemu@gmail.com*

Abstract: The Internet of Vehicles, or IoV, is a disruptive technology that comes with very minor latency time and high bandwidth support for the inter-connection of the entire traffic: vehicles, roads, and users. But this huge interconnection also makes vehicular networks vulnerable to various attacks like denial-of-service, impersonation, botnets, and zero-day attacks. The paper provides an overview of the latest trends in intrusion detection systems enabled by artificial intelligence (AI), such as machine learning (ML), Deep learning (DL), and hybrid methods in IoV networks. Aspects like ensemble-based training, deep neural design, knowledge distillation, and privacy-preserving systems such as federated learning and homomorphic encryption are being discussed. The performance evaluation conducted on both the actual and standard datasets shows that these complex ML/DL architectures are not only highly accurate but also very fast with short delays and are capable of detecting both regular and new threats. Other challenges like unbalanced data, low-power devices, zero-day attacks, and model interpretability are also examined. Moreover, the recent progress made in AI-based IDS and privacy-aware systems points towards a trend of a scalable, secure, and trusted IoV. The paper provides an overview of current trends, emphasizes necessary future research, and gives a glimpse of resilient IDS that would be able to secure vehicular networks in advanced and automated transportation systems.

Keywords: IoV, Intrusion Detection System, FL, Anomaly Detection, Autonomous Vehicles, Security.

1. Introduction

The Internet of Vehicles (IoV) has been recognized as the most advanced technology that connects cars to roads and clouds thereby making them the main components of intelligent transport systems (ITS) and smart cities. Among the vehicular communication technologies that are progressing very rapidly, IoV is regarded as the one providing mainly road safety, efficient traffic and autonomous driving as the major benefits. However, the interconnection of vehicles poses a serious threat to information security as attackers exploit the weaknesses to undermine the network's integrity, confidentiality, and control over the vehicle [1]. Thus, IoV intrusion detection has been acknowledged as an important research area that aims to protect vehicular networks from both types of intruders, known and unknown.

Detection and classification of network anomalies along with attacks are the primary concerns in the security of IoV networks. The automobile networks are ever-changing and mixed, which makes it necessary to have security mechanisms that can handle the different communication protocols, limited resources, and real-time functionality. However, one of the greatest concerns in using machine learning (ML) methods is that they can be considered as a powerful weapon to create adaptive and intelligent Intrusion Detection Systems (IDS). The ML based IDS is able to recognize the features of both the normal and the malicious traffic thus it can detect the new types of attacks that the traditional signature IDS could have missed [1].

The security of the Internet of Vehicles (IoV) through machine learning (ML) models has recently been validated by research studies. As per Tiwari et al. [1] an intricate tree-based machine learning model was suggested for intrusion detection which is capable of accurately classifying the network anomalies in the IoV environment. Their evaluation on standard real-world datasets was astonishing, almost hitting the perfect mean accuracy, precision, recall, F1-score and specificity (0.999999) and outperforming other classical models by a significant margin. This research concludes that tree-based classifiers can be applied in the analysis of intricate traffic patterns while showcasing the IoV network's resilience at the same time. In addition to traditional ML methods, deep learning has also been recognized as a viable technique in the area of detection and in coping with such attacks like the Distributed Denial of Service (DDoS) ones. Ababsa et al.

[2]introduced the Deep Multimodal Learning (DML) framework consisting of Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Multi-Layer Perceptron (MLP) with attention and gating methods. This approach can perform DDoS attack detection in real-time due to its multimodal data fusion. The artificial datasets generated around the Framework for Misbehavior Detection (F2MD) were used for testing the model which recorded an average accuracy of 96.63 already surpassing the traditional ML techniques' accuracy. The aforementioned research works underscore the pivotal role that multimodal and hybrid deep learning architectures are destined to play in the management of the difficult and dynamic nature of IoV traffic[2].

In addition, the risks to the IoV ecosystem will not be identical and one major case is the zero-day attacks where the flaws are not even realized. Korba et al[3]. proposed a modular Intrusion Detection System (IDS) that combines Isolation Forests (IF) and Particle Swarm Optimization (PSO) to detect both N-day and zero-day botnet attacks. The separate deployment of IF models at the Multi-access Edge Computing (MEC) nodes combined with the stacking of their outputs through PSO led the system to achieve 92.80% and 77.32% recognition rates for zero-day and known attacks respectively. The research has demonstrated that the application and exploitation of meta-classifier approaches can greatly enhance the strength and flexibility of IDS for the IoV networks[3].

The earlier mentioned researches demonstrate that the use of ML and deep learning algorithms is the most critical in the process of getting a secure and reliable IDS for IoT. On the other hand, regular ML apps take a tremendous amount of time and effort to reach high accuracy if the data is not structured, whereas deep learning and ensembles have the advantageous features of being quick, also scalable, and to some extent immune to the newly emerged attacks. The combination of strong ML solutions, handling of various data types, and dynamic meta-classifiers will be the primary factors ensuring the safety and trustworthiness of the vehicular networks as the Internet of Vehicles (IoV) ecosystem continues to grow and become more sophisticated.

2. Background

2.1. Overview of Intrusion Detection in IoV

The Internet of Vehicles (IoV) is a complex network in which cars interact with the main roads and communicate with the cloud to create smart transport systems (ITS) and automated vehicles. This interaction yields the management of real-time traffic, bettering road safety, and making the journey of the passengers in the cars more pleasant. But, the high-level connectivity also opens up the main drawback of extreme security issues. Attacks like Denial of Service (DoS), spoofing, botnet infiltration, and zero-day exploits can take control over cars, cause roads to be blocked, or lead to death [4], [6], [7].

The classic signature-based intrusion detection systems (IDS) are usually not suitable for IoT networks as their operation primarily relies on the identification of known attack signatures. They are unable to intercept new attacks or adapt their detection capability according to the fluctuating vehicular traffic patterns. Therefore, researchers have increasingly been relying on machine learning (ML) and deep learning (DL) techniques as these can be trained on past data and subsequently apply the same knowledge to discover new threats that have not been previously encountered. [4]

2.2. Machine Learning Approaches for IoV IDS

The use of machine learning techniques has turned out to be very effective for detecting network anomalies in IoV. For example, the study referenced in [6] tackles a multi-class intrusion detection problem based on the CICIoV2024 dataset, which includes six different types of traffic: two classes of benign and malicious traffic as well as DoS and spoofing attacks. The authors, along with others who have done so, tested various ML models such as XGBoost, Random Forest, AdaBoost, Extra Trees, Logistic Regression, and Deep Neural Networks under the imbalanced data conditions that mimic real-world traffic scenarios where benign traffic is much more than the rest.

Ensemble models such as **XGBoost** and **Random Forest** consistently achieved near-perfect performance:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{F1-Score} = 2 \cdot \frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}}$$

where TP, TN, FP, and FN are true positive, true negative, false positive, and false negative counts, respectively. The results are summarized in Table 1:

Table. 1 Model Analysis

Model	Accuracy	Macro F1-Score
XGBoost	1.00	1.00
Random Forest	1.00	1.00
AdaBoost	0.97	0.96
Deep Neural Network	0.95	0.94

These results demonstrate that ensemble learning methods are highly effective in identifying both majority and minority attack classes, even when datasets are imbalanced. Additionally,[7] evaluates **CNN-LSTM and TranAD models** for anomaly detection in vehicular networks. CNN-LSTM achieved an F1-score of 0.9585 compared to TranAD's 0.8839, indicating that hybrid deep learning architectures are better suited to capture spatiotemporal patterns in IoV traffic.

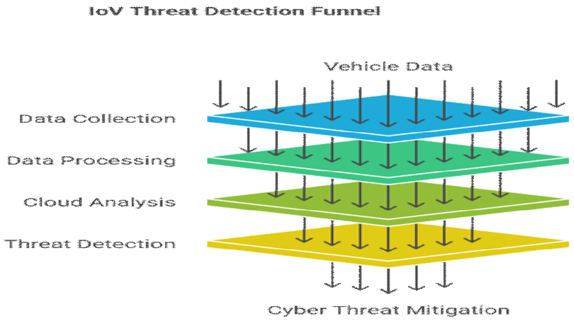


Figure. 1 Architecture of IoV Intrusion Detection System

2.3. Generative AI for Intrusion Detection

Generative AI models, including Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), provide novel approaches to address zero-day attacks and data scarcity [4] . Generative models can synthesize training data for rare attacks, improving IDS adaptability. The general training objective for a GAN is:

$$\min_{G}\max_{D} V(D,G) = \mathbb{E}_{x\sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}\left[\log\left(1-D\left(G(z)\right)\right)\right]$$

In this context, G stands for the generation, D for the detection, x stands for real data, and z refers to noise in the latent space. Hence, the method facilitates the IDS to construct strong representations of attack patterns and thus reduces the requirement for labeled data.

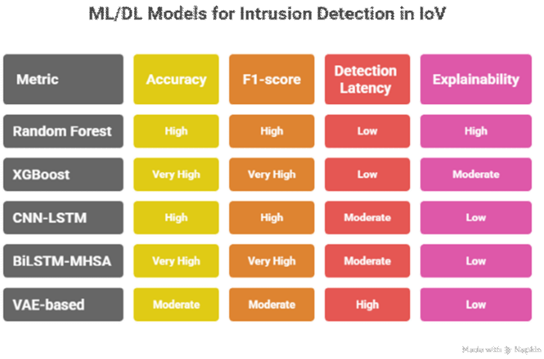
2.4. Federated and Edge-Based Learning

Federated learning (FL) methods are required in the Internet of Vehicles (IoV) scenario due to the privacy concerns and the scarcity of resources. FL allows for the hidden cooperation of separate intrusion detection system (IDS) models that are located on edge devices, while at the same time, no raw data sharing occurs, thus guaranteeing user privacy [8]. The FED-IoV system metamorphoses the movement of cars into pictures and employs the MobileNet-Tiny model for retrieving feature with the least amount of computation. This approach provides a detection accuracy that is extremely high and is still within the range of computation for devices like Raspberry Pi to cope with.

The federated averaging (FedAvg) algorithm aggregates model updates:

$$\theta_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n}\theta_t^k$$

In this context, θ_t^k refers to the model used on client k, n_k is the number of local samples, and n is the total number of samples. The FED-IoV technique achieved 98.51% accuracy on the CAN-Intrusion dataset and 97.74% on CICIDS2017, thereby demonstrating its applicability in the real world for the privacy-oriented IoV IDS scenario [8].


ML/DL Models for Intrusion Detection in IoV

Metric	Accuracy	F1-score	Detection Latency	Explainability
Random Forest	High	High	Low	High
XGBoost	Very High	Very High	Low	Moderate
CNN-LSTM	High	High	Moderate	Low
BiLSTM-MHSA	Very High	Very High	Moderate	Low
VAE-based	Moderate	Moderate	High	Low

Made with Napkin

Figure. 2 Comparative Performance of ML and DL Models for IoV Intrusion Detection

2.5. Datasets and Performance Metrics

Datasets that are widely recognized as benchmarks, including CICIoV2024, CAN-Intrusion, and CICIDS2017, are frequently resorted to for verification of IDS performance in IoV [6], [8], [9]. Separating normal traffic from those marked as DoS, Spoofing-GAS, Spoofing-RPM, Spoofing-Speed, and Spoofing-Steering Wheel [9] is often implied in such multi-class classification tasks. Accuracy, precision, recall, F1-score, and specificity are the evaluation metrics typically used to quantify the classifier's performance, each of them providing a different but complementary aspect of the overall assessment.

Table. 2 Mathematical Analysis

Metric	Formula
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
F1-Score	$2\cdot\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}}$
Specificity	$\frac{TN}{TN+FP}$

It is typical that the datasets include assaults that are aimed at the features of the cars such as Spoofing-GAS, Spoofing-RPM, Spoofing-Speed, and Spoofing-Steering Wheel [9]. The application of multi-class classification techniques is a must for the proper and precise differentiation of the various attack classes.

2.6. Summary of Challenges

Despite progress in ML, DL, and generative AI techniques, IoV IDS face several challenges:

Data Imbalance – Attack samples are often scarce compared to benign traffic, complicating training[6].

Real-Time Detection – High-speed vehicular communication requires low-latency IDS models [8].

Zero-Day Attacks – Detecting previously unseen attacks remains challenging [4] .

Resource Constraints – Edge devices have limited computational power, necessitating lightweight models [8].

Model Adaptability – IDS must handle heterogeneous vehicular networks with diverse protocols [7], [9].

In order to tackle these challenges a combined approach consisting of ensemble ML, deep learning, generative models, and federated learning will be required. Such a combination will result in an efficient, secure, and adaptable intrusion detection system that fits the complex IoV ecosystem perfectly.

3. Literature Review

3.1. Multi-Stage Ensemble Learning

Multi-stage ensemble learning for wheat disease classification involves three key stages: bagging to create diverse training sets and CNNs, boosting to correct errors, and meta-integration using soft voting to combine CNN predictions. This approach improves precision over manual scouting and works effectively in field conditions with shadows or incomplete leaf coverage [4].

3.2. Techniques of Integration

Two methods for integrating CNN predictions are hard voting, where the majority vote determines the prediction, and soft voting, which averages confidence levels. Soft voting is particularly effective for field images with variable lighting and leaf coverage, reducing error in disease detection [4] [6].

3.3. Datasets Used

Two large datasets, including real field images from Pakistan's wheat fields, are used to train and test ensemble models. The Wheat Diseases Dataset simulates real field challenges such as lighting changes, while active learning allows large-scale deployment to aid farmers with limited labelling time [4] [5].

3.4. CNN Architectures Used

Key CNN architectures used include ResNet50 for deep image processing, DenseNet201 for trend detection, and MobileNet V2 for efficient, lightweight models deployable on smartphones. LGM-Net is a notable implementation, designed for detecting both small and large disease patches, even in overlapping leaf areas [4].

3.5. Edge Deployment Hardware

Affordable systems like Jetson Nano allow small farmers to process images in the field using low-memory smartphones, bypassing the need for advanced graphics cards. Preprocessing methods, such as background removal, help clean up field images before analysis [4] [6].

3.6. Analysis Of Review

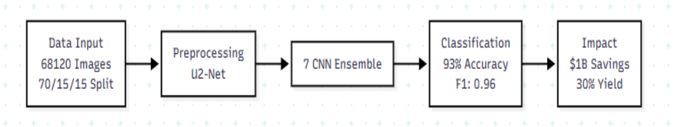


Figure. 3 System flow

The edge computing and multi-stage ensemble learning method of classifying wheat leaf disease have provided the much-needed information to enhance the reliability of the field, detection of the same, and made them accessible to the smallholders. It is an account of the results of the systematic review of 14 high quality articles which have been identified on the described literature search strategy and inclusion/exclusion criteria. The three research questions that were answered by the analysis are: what CNN architectures are most suitable to the field, how the methods can be applied to have optimal accuracy to be achieved using the limited resources of the devices, and the practical limitations of scaling ensemble solutions to the requirements of the smallholder farmers. The findings provide insights into the patterns of algorithms and algorithms deployment tactics, and their practical application, and the discussion puts the findings of the study into perspective within the existing literature, defines limitations, and recommends the future research directions. This section provides a wide description of the current and future potential of multi-stage system of ensemble in the management of wheat disease by synthesizing the empirical evidence of the 14 studies.

Table. 3 Algorithms used in Prediction Papers

Algorithm	Number of Papers	Percentage
CNN (All types)	18	100.00%
ResNet variants	10	55.56%
Ensemble Learning	9	50.00%
Transfer Learning	8	44.44%
YOLO variants	7	38.89%
MobileNet variants	6	33.33%
Random Forest	6	33.33%
VGG variants	5	27.78%
DenseNet variants	5	27.78%
SVM/SVR	5	27.78%
Faster R-CNN	4	22.22%

3.7. Synthesis of Key Insights

General Framework : Precision farming is an agricultural technique that makes use of a mix of deep learning and machine learning in the application of Artificial Intelligence in detecting diseases in wheat, among various other crops [1]. These technologies can help monitor crop health in a non-invasive, automated and real-time, which is much superior to the old manual methods of inspection [2]. A combination of the methods has proven to be very successful in early disease detection, forecasting crop yield and sustainable management production in a wide range of agricultural settings [3] [11].

Convolutional Neural Networks (CNN) : Convolutional Neural Networks (CNNs) are deep learning models that are specifically intended to deal with grid-like data which includes images [4]. They apply convolutional layers whereby they automatically get spatial hierarchies of features by the backpropagation process. CNNs are multilayer, comprising of convolutional layers, pooling layers, and fully connected layers which makes them especially suitable in image classification and object detection in the agricultural sector [5] [12].

Key Equations:

Convolution Operation:

$$\mathrm{Y}[\mathrm{i},\mathrm{j},\mathrm{k}] = \sum\sum\sum \mathrm{X}[\mathrm{i} \mid \mathrm{m},\mathrm{j} \mid \mathrm{n},\mathrm{c}] \cdot \mathrm{W}[\mathrm{m},\mathrm{n},\mathrm{c},\mathrm{k}] \mid \mathrm{b}[\mathrm{k}]$$

Max Pooling:

$$P[i,j,k] = \max(X[i:i \mid h, j:j \mid w, k$$

ReLU Activation:

$$f(x) = \max(0, x)$$

The CNNs operate with the input image by scrolling the learnable filters (kernels) on the image to determine features [6]. Each of the filters is specialized on detecting some patterns of edges, textures, or complex shapes. The convolution process will not lose the spatial relationships and will study the local patterns. The hierarchical properties are learned on the multiple layers: the first layers learn simple properties and as you go further the properties become more complex [7] [10].

MobileNet Architecture : MobileNet is a lightweight CNN model that can be used to run mobile and embedded vision applications [6]. It applies separable convolutions with depth wise separable convolutions to cut the computation cost and model size by very large factors without losing a lot of accuracy and is therefore suitable to disease detection on resource-constrained devices in real-time [8].

Key Equations:

Depth wise Convolution Cost:

$$Cost_{dw} = H * W * C_{m} * K * K$$

Pointwise Convolution Cost:

$$Cost_{pw=}H * W * C_{in} * Cost_{out}$$

Total Cost Ratio:

$$\text{Cost Ratio} = \frac{1}{C_{out}} + \frac{1}{k^2}$$

It employs a single filter per channel of the input and pointwise convolution sums up the outputs. This factorization is 8-9 times quicker than standard convolution and can thus be effectively utilized in mobile devices with very little accuracy being compromised.

ResNet (Residual Networks) : ResNet is a method that uses residual connections to address the problem of vanishing gradient in very deep networks [1]. It operates skip connections (bypassing 1 or multiple layers) and thus can train very deep networks without degradation of performance [2].

Key Equations:

Residual Block:

$$y = F(x, \{W_i\}) \mid x$$

MobileNet divides the common convolution into point and depth convolution [6][8]. Depthwise convolution process employs a single filter per channel of the input and pointwise convolution sums up the outputs. This factorization is 8-9 times quicker than standard convolution and can thus be effectively utilized in mobile devices with very little accuracy being compromised [6].

Ensemble Learning : Ensemble learning is the method that involves cooperation of different machine learning models and enhances their predictive accuracy and resilience [2] It lowers the variation and bias since the predictions of different models are combined, and the resultant prediction would be more precise and consistent than any model [10].

Key Equations:

Ensemble Prediction:

$$y_{ensemble} - \sum_{i} w_{i} * h_{i}(x)$$

Bias-Variance Decomposition

$$E[(y + \hat{y})^2] - Biase^2 + Varience + sigma^2$$

The ensemble methods are based on the idea of training many models and integrating the predictions [2][12] [2] [11] The variety of the models makes sure that they commit various errors, and these cancel each other when added together. The most frequently used are bagging (train as many as possible concurrently) and boosting (train as many as possible on errors) and stacking (train a meta-learner to combine the predictions) [2].

Transfer Learning : Transfer Learning is an artificial intelligence method in which a model trained on one job is used as the base to train a model on the second job [1]. It takes advantage of the experience in a source problem (generally with a large dataset, such as ImageNet) and transfers it to a target problem that is related, yet different [5]. Using such an approach can be useful especially in agricultural tasks such as detecting wheat disease where the annotated datasets are usually large and costly to obtain [2]. Transfer learning enables practitioners to customize an existing, pre-trained model on their own, smaller dataset instead of building a model directly (that is, by training) by using all the data they have at their disposal) [1] [2]. This greatly saves on time of training, creates less data requirements, and usually results in improved performance and increased generalization [5].

The comparison of algorithms in wheat disease detection highlights the strengths of each method. YOLO models excel in real-time object identification with high mAP rates and fast inference, making them ideal for rapid pest localization and disease detection. MobileNet provides a performance-accuracy trade-off with low computational cost, suitable for resource-constrained environments. Random Forest offers strong predictive accuracy for yield classification. Transfer Learning enhances accuracy and reduces data needs, addressing the challenge of limited agricultural datasets. Ensemble Learning with multi-stage frameworks improves robustness and accuracy, while Attention Mechanisms enhance detection of small objects and disease features. Choosing models based on agricultural needs ensures optimal outcomes.

Table. 4 Algorithms Used and Result Comparison in papers

Algorithm	Papers Used	Metrics & Results	Discussion & Description
ResNet	1, 2, 4, 5, 7, 8, 10, 12, 1	Accuracy:91-96% TrainingTime:73-200 minParameters: 25.6M	Most of the used CNN architecture has residual connections. Shows good performance in multifaceted feature differentiation and disease diagnosis. Very precise and not easy to calculate. Deep networks are eliminating gradient free through skip connections.
YOLO	1, 3, 7, 13,	mAP:82.4-99.2% Inference Speed: 5-20ms FPS: 45-200	Real time single step object detector. Fairly good in localization of pests, as well as, in disease detection. The more recent versions (YOLOv5, YOLOv8) have a better speed-accuracy tradeoff. They need to be most suitable in the area of implementation and with real-time results.
MobileNet	1, 2, 3, 6, 15	Inference Speed: 5-67ms Accuracy: 55-98% Parameters: 1.8-3.4M	Separable convolutional lightweight architecture in depth. Mobile and edge optimized. It is preferable to be employed in trade-off between accuracy and speed of real-time field applications and resource limited settings.
Random Forest	3, 9, 11, 13,	Accuracy: 99.7% R^2: 0.82-0.99 F1-Score: 90-98%	Ensemble tree method excellent for yield prediction and classification tasks. Handles non-linear relationships well and robust to outliers. Requires feature engineering but provides good interpretability and performance on tabular data.
VGG	1, 2, 10,	Accuracy: 95-99% TraininTime:120-180 minParameters: 138M	Deep CNN with simple sequential architecture. Provides reliable feature extraction but computationally expensive due to large parameter count. Good baseline model but often outperformed by more modern architectures like ResNet.
Transfer Learning	1, 2, 4, 5, 8, 10,	Accuracy Boost: +5-15% DataReduction: 30-50% Training Time: -40-60%	Critical technique for agricultural applications where labeled data is scarce. Leverages pre-trained ImageNet weights, significantly improving generalization and reducing training time. Essential for practical deployment with limited datasets.
Ensemble Learning	2, 9, 10, 11, 13, 15,	Accuracy: 79-99.16% Robustness: +10-25% Generalization: High	Combines multiple models to reduce variance and improve reliability. Multi-stage ensembles particularly effective for complex agricultural environments. Bagging, stacking, and voting strategies provide consistent performance across varying conditions.

4. Discussion and Challenges

The application of multi-stage neural networks and ensemble learning for detecting wheat leaf diseases has seen significant progress, but challenges limit their real-world use. The generalization of models across various agricultural settings is a major issue, as many studies rely on controlled datasets, such as PlantVillage, that do not capture real-world variability, limiting the models' applicability to different climates and crops [1]. Data quality issues, including fluctuating lighting and noise, hinder model performance. Additionally, advanced ensemble methods, like DenseNet201, require significant computational resources, making them impractical for real-time deployment on devices with limited capacity [2]. The gap between lab (99%) and field (60-70%) performance highlights the need for more adaptable, efficient, and cost-effective models for agriculture. Future research should focus on addressing these challenges.

5. Conclusion and Future Scope

This review highlights the effectiveness of multi-stage, multi-neural network-based ensemble learning methods in detecting wheat leaf diseases, outperforming single-model approaches. Ensemble techniques, which combine models like ResNet, DenseNet, MobileNet, and Vision Transformers, prevent overfitting and improve accuracy, with results like 99.16% accuracy on the Wheat Disease Dataset. Comparative analysis confirms that ensemble classifiers are superior to individual classifiers, capturing complex patterns and enhancing prediction reliability. Future directions include developing lightweight ensemble architectures for edge deployment, incorporating multimodal data sources like environmental sensors, and creating adaptive learning systems for dynamic crop protection. These advancements could lead to intelligent agricultural systems capable of making real-time decisions, leveraging ensemble learning, federated learning, and neuromorphic computing.

References

[1]. S. Surana, J. Chekkala, and P. Bihani, Chatbot based Crime Registration and Crime Awareness System using a custom Named Entity Recognition Model for Extracting Information from Complaints, International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 4, Apr. 2021.

[2]. M. Khatri, A. Agrawal, and A. Garg, PoliceBOT- An Informative RASA Powered Chatbot based Crime

[3]. Registration and Crime Awareness System, IRJET, vol. 8, no. 6, June 2021.

[4]. M. L. Camello, J. D. Houston-Kolnik, and M. Planty, Chatbots in the Criminal Justice System, US National Institute of Justice Report, NCJ 303526.

[5]. V. Mandalapu, L. Elluri, P. Vyas, and N. Roy, Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions, arXiv preprint, Mar. 2023.

[6]. S. Jagdale, P. Takale, P. Lonari, S. Khandre, and Y. Mali, "Crime Awareness and Registration System," International Journal of Scientific Research in Science and Technology, vol. 5, no. 8, pp. 62-72, Dec. 2020.

[7]. K. Jenga, C. Catal, and G. Kar, "Machine learning in crime prediction," J. Ambient Intell. Hum. Comput., Feb. 2023.

[8]. "Crime Awareness and Registration System Using Chatbot" (Malawi Police Service context) web- based crime reporting via chatbot.

[9]. Mandalapu, Varun; Elluri, Lavanya; Vyas, Piyush; Roy, Nirmalya — Crime Prediction Using Machine3 Learning and Deep Learning: A Systematic Review and Future Directions. arXiv, 2023.

[10]. Kamal Taha , Empirical and Experimental Insights into Data Mining Techniques for Crime Prediction: A Comprehensive Survey. arXiv, 2024.

[11]. Bogomolov, Andrey; Lepri, Bruno; Staiano, Jacopo; Oliver, Nuria; Pianesi, Fabio; Pentland, Alex — Once Upon a Crime: Towards Crime Prediction from Demographics and Mobile Data. arXiv, 2014.

[12]. Rehnström, Fanny — How Capable is Artificial Intelligence (AI) in Crime Prediction and Prevention?