

Guarding the Digital Harvest: An AI/ML-Based Intrusion Detection Framework for Agriculture 4.0 Networks

Varun K S

Department of Computing and IT,
GM University, Davanagere, Karnataka, India
varunksbennur@gmail.com

Rahul V

Department of MCA,
G M University, Davanagere, Karnataka, India
rahultech422@gmail.com

Abstract: Agriculture 4.0 is transforming modern farming practices. It uses Internet of Things devices, smart sensors, drones, automated irrigation systems, and cloud-based technologies. These new technologies help farmers improve operational efficiency and use resources wisely. However, they also make Agriculture 4.0 networks more vulnerable to cyberattacks. Various types of attacks can disrupt agricultural operations, such as Distributed Denial-of-Service attacks, Port Scanning, Botnet activities, and Brute Force intrusions. These attacks can disrupt farming operations and put important Agriculture 4.0 data at risk. Traditional intrusion detection methods mostly look for known threats and often miss new or unknown ones. This study proposes a Machine Learning-based Intrusion Detection System (IDS) for Agriculture 4.0 environments using the Random Forest algorithm. The Farm Flow dataset containing agricultural network traffic was utilized for training and evaluation. Data preprocessing techniques, including feature selection, label encoding, and normalization, were applied to improve model performance. The proposed system identifies whether network traffic is normal or associated with attacks such as DDoS, Port Scan, Botnet, or Brute Force. The system was evaluated using performance metrics such as accuracy and precision, along with a confusion matrix. The results show that using machine learning can effectively enhance the security of farming systems against cyberattacks by detecting malicious activities quickly and accurately. Furthermore, the proposed system provides a cost-effective approach for securing Agriculture 4.0 systems.

Keywords: Agriculture 4.0 Cybersecurity, Intrusion Detection System, Machine Learning, Random Forest, IoT Security, Smart Farming, Artificial Intelligence.

Nomenclature

Abbreviation	Description
AI	Artificial Intelligence
IoT	Internet of Things
DDoS	Distributed Denial-of-Service
IDS	Intrusion Detection System
ML	Machine Learning
ML-IDS	Machine Learning-Based Intrusion Detection System
RF	Random Forest
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
KNN	K-Nearest Neighbors
SVM	Support Vector Machine
Agri-IoT	Agricultural Internet of Things
WSN	Wireless Sensor Network
XAI	Explainable Artificial Intelligence

1. Introduction

Agriculture has undergone significant transformation through the adoption of advanced technologies, leading to the emergence of Agriculture 4.0. This new approach to agriculture incorporates technologies such as devices that can connect to the internet, cloud-based computing, artificial intelligence, machine learning, wireless sensors, and automated systems to make farming better and more sustainable. The integration of these technologies enables agricultural activities to become more connected, automated, and data-driven. Farmers can now monitor crop health, automatically control irrigation systems, monitor weather and other environmental conditions, and make decisions based on the information they have in

real time. These capabilities can help farmers improve productivity, manage resources efficiently, and respond more quickly to changes in agricultural conditions. The increasing integration of IoT and AI technologies in agriculture also introduces new cybersecurity requirements [1][3]. With all these benefits, the fact that agricultural systems are connected to the internet has brought up new challenges related to cybersecurity and information security. The devices used in farming are always receiving and transmitting information over networks that can be accessed by external users. As the number of connected agricultural devices continues to increase, the potential attack surface of Agriculture 4.0 environments also becomes larger. Malicious actors attempting to gain unauthorized access to these networks can exploit vulnerabilities and launch attacks that may disrupt system operations, compromise information, or reduce system efficiency [2].

There are various types of cyberattacks that pose security concerns for farmers, including Distributed Denial-of-Service (DDoS) attacks, Port Scanning, Botnet activities, and Brute Force attacks [1][4]. In Agriculture 4.0 environments, such attacks can affect not only communication networks but also connected sensors, automated equipment, data management systems, and other smart farming components. These are concerns for farmers who use smart farming techniques. The consequences of these attacks may include service disruption, unauthorized access, data loss, and reduced reliability of automated agricultural operations. Traditional intrusion detection systems are generally based on predefined attack signatures and fixed security rules. While effective against known threats, they are unable to identify previously unseen attack patterns and evolving cyber threats. This creates a need for security systems that are intelligent and can learn from network behavior and adjust to new attack strategies. An intelligent intrusion detection mechanism is therefore important for continuously monitoring agricultural network traffic and identifying suspicious activities that may not match previously defined attack signatures. Agricultural IoT devices and Agriculture 4.0 infrastructures therefore require intelligent security mechanisms capable of learning from network behavior and adapting to emerging attack strategies [3][5].

Machine Learning provides a potential approach for addressing these security challenges. Machine Learning can analyze network traffic patterns and distinguish between normal and malicious activities with high accuracy. By analyzing network traffic characteristics, Machine Learning techniques can learn relationships between network features and different types of malicious activities. This capability can support the detection of both normal network behavior and abnormal patterns associated with cyberattacks. In this context, this research proposes a system that uses the Random Forest algorithm for attack detection in technologically advanced agricultural environments using data obtained from agricultural networks. The use of a suitable Machine Learning algorithm can improve the ability of an intrusion detection system to classify network traffic according to its observed characteristics. The Random Forest algorithm is employed to analyze network traffic features and classify network activities according to their corresponding behavioral patterns.

The system uses Machine Learning, and it looks at network traffic patterns to distinguish between normal and malicious activities with high accuracy. Such a system can assist in identifying malicious network behavior and strengthening the security of connected agricultural environments. The research presents a system that uses Random Forest to find attacks, and it is made for Agriculture 4.0 environments using data from agricultural networks. The proposed approach focuses on analyzing agricultural network traffic and identifying whether the observed traffic represents normal activity or an attack. The system is intended to provide an intelligent and practical security mechanism for Agriculture 4.0 environments, where the protection of connected devices, network communication, and agricultural data is increasingly important. Therefore, the application of Machine Learning-based intrusion detection can contribute to improving the reliability and security of modern agricultural systems while supporting the continued adoption of Agriculture 4.0 technologies. The proposed Random Forest-based intrusion detection system is therefore intended to enhance the capability of Agriculture 4.0 environments to detect malicious network activities and provide improved protection for connected agricultural infrastructure.

2. Literature Review

Table 1 summarizes existing AI/ML-based intrusion detection studies, their methods, findings, and identified research gaps.

Table 1. Summary of Existing Machine Learning and Artificial Intelligence-Based Intrusion Detection Approaches for Agriculture 4.0 and Related IoT Environments

No	Title	Authors	Objective	Method	Key Findings	Gap Identified
1	Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions	Ferrag et al. [1]	Review AI/ML-based IDS solutions for Agriculture 4.0	Systematic survey of ML, DL, IDS datasets and frameworks	AI-based IDS significantly improves attack detection in smart farming environments	Lack of agriculture-specific datasets and real-world deployments
2	AI-Based Detection of Cyber Intrusions in Food Supply Chains and Agricultural IoT Networks	Layla Keating [2]	Investigate techniques for intrusion detection in Agri-IoT and food supply chains.	AI Supervised ML, Unsupervised ML, CNN, RNN, LSTM, and Autoencoders	AI enables real-time detection, anomaly recognition, and proactive cyber defense	Limited large-scale datasets, lightweight models, and continuous learning frameworks
3	Securing the Internet of Things: The Role of Artificial Intelligence in Agricultural Cyber Defense	Dora Konstantinou et al. [3]	Examine AI applications for improving agricultural IoT security	AI-driven ML, predictive analytics	IDS, DL, AI outperforms traditional IDS for detecting zero-day attacks and advanced threats.	Scalability and integration challenges in agricultural environments
4	Intrusion Detection System for Securing Agriculture 4.0 against DDoS Attacks using Deep Learning and Machine Learning Models	Mohammad Mirmarghabi, Ahmad Afshar, Hajar Atrianfar [4]	Develop an IDS to detect DDoS attacks in Agriculture 4.0	KNN, RF, Logistic Regression, Neural Networks, CNN using CICIDS2017 dataset	CNN achieved the highest detection accuracy among evaluated models	Focused mainly on DDoS; broader attack categories remain underexplored
5	An AI/ML Framework for Proactive Cyber Threat Detection in Uncrewed Aerial Vehicles	Ogunfowora & Panday	Design adaptive IDS for UAV cybersecurity	Kalman Filter, Supervised Learning, Reinforcement Learning, Blockchain Logging	Hybrid IDS improves adaptability and proactive threat detection in UAVs	Framework evaluated primarily in simulation environments
6	Current Trends in AI and ML for Cybersecurity: A State-of-the-Art Survey	Nachaat Mohamed [5]	Review AI and ML applications in cybersecurity	Comprehensive literature survey	Intrusion detection, malware detection, and network security are key AI applications.	Ethical issues, explainability, data privacy, and implementation costs remain challenges.
7	Cybersecurity Intrusion Detection in Industry 4.0 WSNs Using ML/DL	Chappidi Suneetha et al. [6]	Develop intrusion detection for Industry 4.0 Wireless Sensor Networks.	Stacking Classifier, XGBoost, AdaBoost ensemble learning	Ensemble methods improved accuracy and reduced false positives	Not specifically designed for agricultural IoT environments
8	Explainable AI-based Intrusion Detection System for Industry 5.0	Naseem Khan et al. [7]	Review Explainable AI (XAI) for IDS in Industry 5.0	XAI-based taxonomy survey	IDS XAI improves transparency, trust, and interpretability of AI-based IDS	Vulnerability to adversarial attacks and lack of mature XAI frameworks
9	The Role of AI in Cybersecurity: A Cross-Industry Model for Integrating Machine Learning and Data Analysis for Improved Threat Detection	Favour Uche Ojika et al. [8]	Develop cross-industry AI-driven cybersecurity framework.	Supervised ML, Unsupervised ML, Big Data Analytics, SIEM integration	AI improves anomaly detection, threat intelligence, and response time	Explainability and interoperability issues across sectors
10	Agricultural IoT Security and AI-Based Intrusion Detection Systems (from uploaded Agriculture 4.0 review collection)	Various Authors (reviewed in RRP set)	Analyze AI-based IDS frameworks in agricultural environments	Hybrid ML/DL architectures and anomaly detection approaches	AI-enhanced IDS achieves >90% accuracy in simulated agricultural networks	Limited real-world validation and lack of benchmark agricultural datasets

3. AI Techniques for Intrusion Detection in Agriculture 4.0

Artificial Intelligence and Machine Learning provide advanced capabilities for identifying malicious activities within agricultural networks. The increasing connectivity of agricultural IoT devices, sensors, automated systems, and cloud-based platforms has created a need for intelligent techniques capable of detecting and classifying cyber threats. The most commonly applied techniques include Supervised Machine Learning, Unsupervised Machine Learning, Deep Learning, and Hybrid AI models. These techniques differ in their learning mechanisms, data requirements, and ability to detect known and previously unseen cyberattacks.

3.1 Supervised Machine Learning

Supervised learning algorithms are trained using labeled datasets that include malicious network traffic. These datasets help the algorithms learn the characteristics of normal and malicious network activities. After training, the models classify new network traffic according to the patterns learned from the labeled data. Examples include:

- Random Forest (RF)
- Decision Tree (DT)
- Support Vector Machine (SVM)
- Logistic Regression (LR)
- K-Nearest Neighbors (KNN)
- XGBoost

The algorithms then use this knowledge to classify network behavior based on what they have learned. They are particularly effective at detecting attacks that are already known. Supervised learning is widely used in intrusion detection because its classification capability can provide high detection accuracy when sufficient and representative labeled training data are available. However, its performance may depend on the quality, diversity, and relevance of the training dataset.

3.2 Unsupervised Machine Learning

Unsupervised learning techniques identify patterns and structures in network traffic without requiring predefined class labels. Common methods include:

- K-Means Clustering
- DBSCAN
- Principal Component Analysis (PCA)
- Autoencoders

They can anomalous or abnormal network activities without needing a dataset that has labels on it. This characteristic makes unsupervised learning useful for identifying previously unknown or evolving attack patterns, particularly when labeled agricultural network traffic is limited.

3.3 Deep Learning Techniques

Deep learning models can learn patterns in large-scale network traffic datasets with minimal manual feature engineering. These models can automatically extract complex features from network traffic and identify relationships that may be difficult to capture using conventional Machine Learning algorithms. Popular architectures include:

- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)
- Long Short-Term Memory (LSTM)
- Deep Neural Networks (DNN)

Deep learning models usually do a better job of detecting complex and evolving attack patterns than traditional machine learning algorithms [4][9]. However, deep learning approaches generally require larger datasets, higher computational resources, and careful model training, which can present challenges for resource-constrained agricultural IoT environments.

3.4 Hybrid AI Models

Some models use more than one technique to get better results. Hybrid AI models combine the complementary capabilities of multiple algorithms to improve the accuracy, robustness, and adaptability of intrusion detection systems. Examples include:

- CNN-LSTM
- Autoencoder + Classifier

- Random Forest + XGBoost
- Ensemble Learning Models

These methods use the strengths of multiple algorithms to make intrusion detection better. By combining different learning techniques, hybrid models can improve the detection of complex attack patterns and reduce the limitations associated with individual algorithms. Such approaches are particularly relevant to Agriculture 4.0 environments, where network traffic can originate from diverse devices and applications with different communication characteristics.

4. Challenges and Research Gaps

Even though significant progress has been made in the application of Artificial Intelligence for intrusion detection, there are still several challenges that limit the effective deployment of AI-based security solutions in Agriculture 4.0. These challenges are related to data availability, computational resources, detection capability, explainability, scalability, and real-world validation.

4.1 Limited Agricultural Datasets

Most studies use general cybersecurity datasets, like CICIDS2017, NSL-KDD, and UNSW-NB15, which do not adequately represent the characteristics of agricultural environments. The lack of agriculture-specific datasets containing realistic network traffic and diverse cyberattack scenarios limits the development and evaluation of reliable intrusion detection models for Agriculture 4.0.

4.2 Resource Constraints

Agricultural IoT devices do not have a lot of power to process information; they do not have a lot of memory, and their batteries do not last long. These resource limitations make it difficult to deploy computationally intensive Artificial Intelligence and Machine Learning models directly on agricultural IoT devices. This makes it hard to use models that can learn and understand things on these Agricultural IoT devices. Therefore, lightweight and computationally efficient intrusion detection models are required for resource-constrained agricultural environments.

4.3 Detection of Zero-Day Attacks

Lots of systems that are supposed to find and stop attacks have a hard time figuring out new attack patterns that they have never seen before. These systems are often not good at detecting Zero-Day Attacks on Agricultural IoT devices. The primary challenge is the inability of conventional intrusion detection approaches to recognize previously unseen attack behaviors.

- They have trouble with Zero-Day Attacks.
- They have trouble with attack patterns.

This is a big problem for Agricultural IoT devices because they are often the target of Zero-Day Attacks. The ability to identify previously unknown threats is therefore important for protecting connected agricultural infrastructure from evolving cyberattacks. Systems that look for anomalies might think normal activities are bad, which leads to warnings and disruptions.

4.4 False Alarms Are A Big Problem

False alarms happen when systems that look for anomalies think something normal is actually bad, and that causes a lot of work and problems. A high false-positive rate can generate unnecessary security alerts, increase the workload of security administrators, and potentially disrupt legitimate agricultural operations. Therefore, reducing false alarms while maintaining high detection accuracy remains an important research challenge.

4.5 Lack of Explainability

Artificial intelligence models are like black boxes, so security analysts have a hard time understanding why they make certain decisions. The lack of transparency and interpretability can reduce trust in AI-based intrusion detection systems, particularly when security decisions need to be verified or investigated. Explainable Artificial Intelligence (XAI) techniques can help provide insights into the features and patterns that influence the model's predictions. This issue is separate from the resource constraints discussed in Section 4.2 and is therefore removed to avoid repetition.

4.6 Scalability Issues

Agriculture 4.0 environments can contain a large and continuously increasing number of IoT devices, sensors, gateways, and connected systems. As the number of devices and network traffic increases, intrusion detection systems must be capable of processing large volumes of data while maintaining detection performance. Therefore, scalability remains an important challenge for deploying AI-based intrusion detection systems across large agricultural environments.

4.7 Real-World Validation

Most proposed solutions are evaluated using simulated environments rather than real agricultural deployments. Although simulation-based evaluation is useful for initial testing, it may not fully represent the network behavior, device limitations, environmental conditions, and security requirements of real-world agricultural systems. The use of realistic IoT datasets can provide a more representative basis for evaluating network intrusion detection and security mechanisms [10]. Therefore, real-world validation using agriculture-specific network traffic and operational environments is required to establish the reliability and practical applicability of proposed intrusion detection systems.

5. Proposed System

5.1 System Overview

Building on the gaps identified in the previous sections, this study proposes a Machine Learning-based Intrusion Detection System (ML-IDS) specifically for Agriculture 4.0 networks. Instead of matching traffic against a fixed list of known attack signatures, conventional signature-based systems do, the proposed system analyzes patterns in network traffic and classifies the observed traffic as either normal or one of four attack categories: DDoS, Port Scan, Botnet, or Brute Force.

The core of the system is based on a Random Forest Classifier. The Random Forest algorithm was selected because it is well suited for structured and tabular network data. It can also handle complex network traffic patterns while maintaining robust classification performance. The Random Forest Classifier also offers relatively low computational complexity compared with many deep learning models, making it suitable for resource-constrained smart farming environments. Therefore, Random Forest was selected as the primary classification algorithm for the proposed ML-IDS because of its simplicity, robustness, and suitability for network traffic classification.

5.2 Dataset Description

The system is trained and evaluated on the Farm Flow dataset, a collection of agricultural network traffic records covering both normal activity and the four attack types mentioned above. Each row in the dataset represents a single network flow and carries attributes such as packet size, flow duration, protocol type, byte and packet counts, and traffic rate, all of which help the model separate legitimate farm traffic from malicious activity.

The Farm Flow dataset was selected because it represents agricultural network traffic rather than relying solely on general-purpose cybersecurity datasets such as NSL-KDD and CICIDS2017. The use of agriculture-specific traffic is important because general cybersecurity datasets may not adequately represent the communication characteristics and network behavior of Agriculture 4.0 environments.

5.3 Data Preprocessing

Raw network traffic data is rarely ready to be fed straight into a model, so before training began we ran the dataset through a few preprocessing steps:

- **Handling Missing Values:** Rows with null or incomplete fields were cleaned so they would not distort training.
- **Label Encoding:** The target attack categories (Normal, DDoS, PortScan, Botnet, Bruteforce) were converted into numeric labels the model could work with.
- **Removing Irrelevant Columns:** Fields that did not contribute useful information, such as identifiers, were dropped.
- **Feature Scaling:** Numeric features were scaled so that columns with numbers did not have too much influence on the model.
- **Train-Test Split:** The data was divided into a part for training and a part for testing so the model could be checked on data it had never seen before.

These preprocessing steps were applied consistently to ensure that the input data were suitable for model development and subsequent intrusion detection.

5.4 Model Development

Random Forest works by creating decision trees during the learning process. Each tree produce a classification decision, and the final prediction is determined by combining the decisions of the individual trees. This ensemble mechanism reduces the influence of individual noisy or overfitted decision trees and improves the overall robustness of the classifier.

This behavior suits intrusion detection well, since network traffic patterns can vary quite a bit even within the same attack category, and an ensemble approach is generally better at generalizing across such variations. The Random Forest model was trained using the preprocessed Farm Flow features to classify incoming traffic into five classes: Normal, DDoS, PortScan, Botnet, and Bruteforce. The trained model, along with the scaler and label encoder used during preprocessing, was saved so that it could be reused for prediction without requiring retraining each time.

5.5 System Architecture and Workflow

The system was built as a pipeline made up of the following stages:

- **Data Collection:** Agricultural network traffic is gathered from the Farm Flow dataset.
- **Data Exploration:** The dataset is examined to see understand its characteristics, identify missing information, and analyze the distribution of traffic across different classes.
- **Data Preprocessing:** The data are cleaned, encoded, scaled, and divided into training and testing subsets.
- **Model Training:** The Random Forest Classifier is trained on the processed training data.
- **Model Evaluation:** The trained model is evaluated using the testing dataset and the performance metrics.
- **Intrusion Detection and Prediction:** Previously unseen network traffic is subjected to the same preprocessing procedures, and then provided to the trained model for classification.
- **Attack Classification:** The model classifies each network flow as Normal, DDoS, PortScan, Botnet, or Bruteforce.
- **Results and Output:** The classification results are summarised and saved in a CSV file along with a report of the detected intrusions.
- **Alert and Response:** When an attack is detected, the system can flag the suspicious activity and notify an administrator for further investigation and response.

The trained model, scaler, and label encoder were stored in accessible locations so that the prediction engine could retrieve them efficiently whenever new network traffic required classification, rather than training a new model for every prediction. This workflow enables the proposed system to perform consistent preprocessing, classification, and reporting throughout the intrusion detection process. The fig. 1 illustrated the proposed methodology.

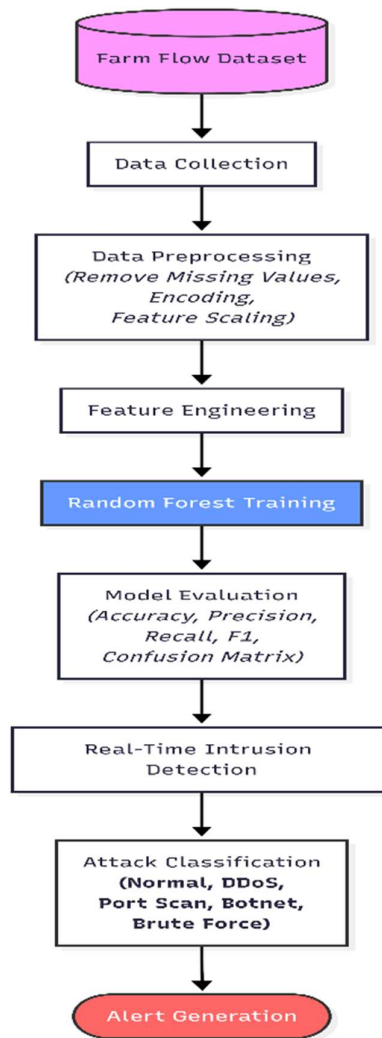


Fig. 1. Proposed Machine Learning-Based Intrusion Detection Framework for Agriculture 4.0 Using the Farm Flow Dataset and Random Forest Classifier.

5.6 Evaluation Metrics

- **Accuracy:** The overall proportion of network traffic samples that are correctly classified.
- **Precision:** The proportion of samples that predicted as attacks that are actually attacks, indicating the reliability of the generated alerts.
- **Recall:** The proportion of the actual attack samples that are correctly detected, indicating the system's ability to identify malicious activities.
- **F1-Score:** The harmonic mean of precision and recall, providing a balanced measure of classification performance, particularly when class distributions are unequal.
- **Confusion Matrix:** A detailed comparison between predicted and actual class labels that helps identify classification errors and determine which attack categories are most frequently confused with one another.

5.7 Key Advantages of the Proposed System

- Can flag both known attack types and traffic patterns it has not explicitly memorized, since it learns general patterns rather than fixed signatures.
- Handles multi-class classification, differentiating between DDoS, Port Scan, Botnet, and Brute Force instead of just a simple normal-versus-attack choice.
- Runs smoothly on hardware, which matches the resource limits often found in agricultural IoT setups.
- Built using open-source tools (Python, Scikit-Learn, Pandas), keeping costs for deployment and maintenance low.

5.8 Limitations of the Current Implementation

The proposed system has its limitations, several of which match the broader challenges mentioned earlier. It is. Tested on a single dataset (Farm Flow) instead of traffic taken from multiple real farms, so its performance on truly new real-world situations still needs to be tested. Testing was also done offline on data instead of on live network traffic, so the speed and ability to handle data in real-time conditions have not been checked yet. These limitations are addressed further in the future research directions below.

6. Experimental Results and Discussion

The proposed Random Forest-based Intrusion Detection System was evaluated using the Farm Flow dataset. The model was trained on preprocessed agricultural network traffic and tested using a separate testing dataset. Model performance was assessed using a confusion matrix, feature importance analysis, and attack distribution visualization. These experiments demonstrate the capability of the proposed model to classify multiple attack categories effectively in Agriculture 4.0 environments.

6.1 Attack Type Distribution

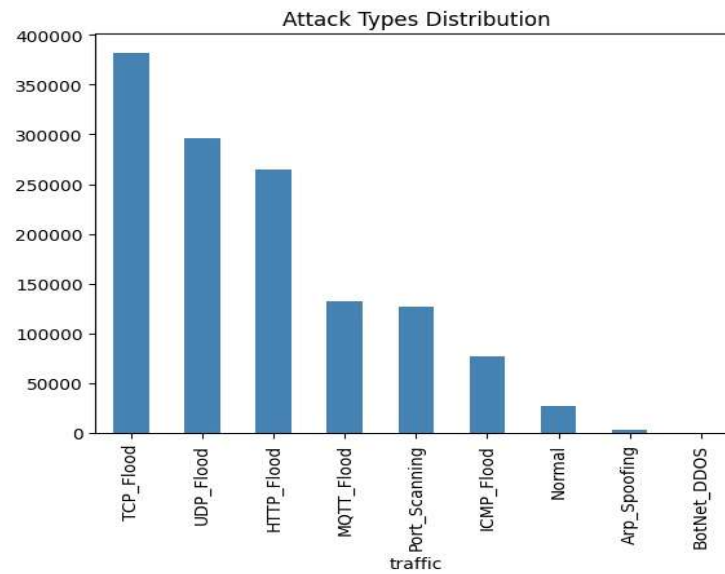


Fig. 2. Distribution of attack classes in the Farm Flow dataset.

Fig. 2 presents the distribution of attack categories in the Farm Flow dataset used for this study. The dataset includes both network traffic and several types of malicious traffic, including TCP Flood, UDP Flood, HTTP Flood, MQTT Flood, ICMP Flood, ARP Spoofing, BotNet DDoS, and Port Scanning attacks. TCP Flood and UDP Flood make up the parts of the dataset, while BotNet DDoS and ARP Spoofing have much fewer examples. The fact that there is a distribution of classes shows real-world network situations and shows why it is important to use a strong ensemble classifier, like Random Forest.

6.2 Feature Importance Analysis

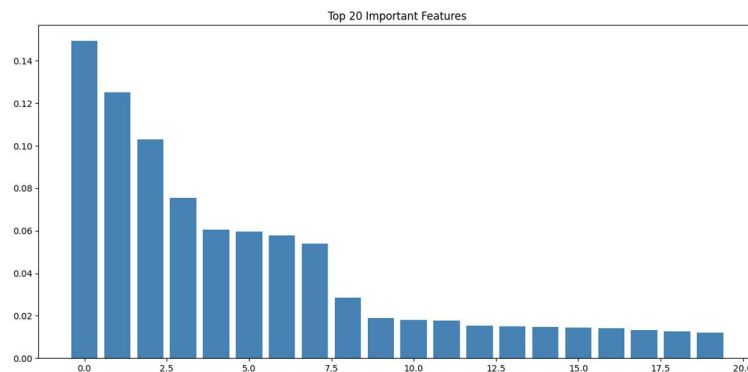


Fig. 3. Top 20 most important features identified by the Random Forest classifier.

Fig. 3 illustrates the twenty most influential features used by the Random Forest classifier during intrusion detection. Feature importance was calculated using the Gini importance measure. The first few features contribute significantly more to the classification process than the remaining features, indicating that only a subset of network attributes is highly discriminative. This observation also suggests that future work could incorporate feature selection techniques to reduce computational complexity without sacrificing detection performance.

6.3 Confusion Matrix Analysis

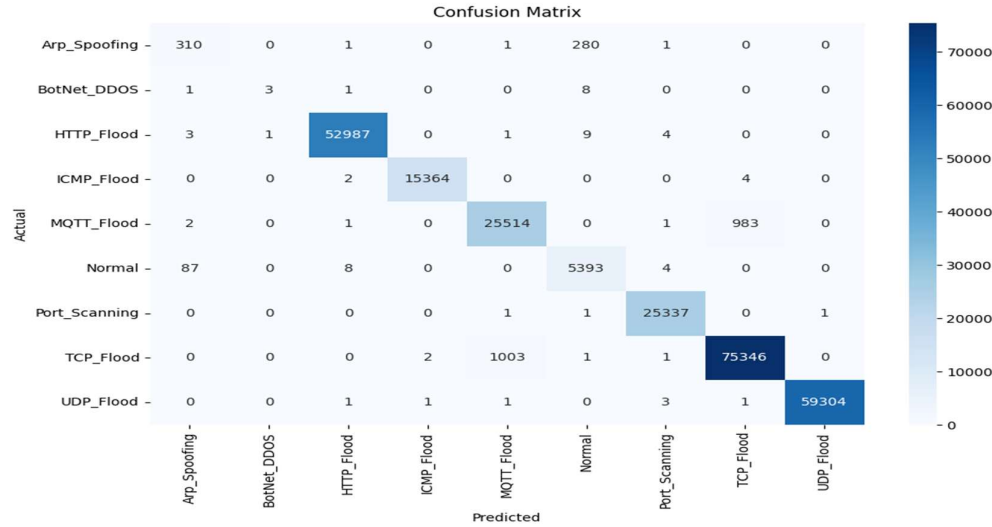


Fig. 4. Confusion matrix of the proposed Random Forest intrusion detection model.

Fig. 4 shows the confusion matrix that came from the Random Forest classifier. Most attack classes are correctly identified, as shown by the numbers on the main diagonal. The model does a good job of recognizing TCP Flood, UDP Flood, HTTP Flood, ICMP Flood, and Port Scanning attacks. A small number of misclassifications are observed between Normal traffic and ARP Spoofing, as well as between MQTT Flood and TCP Flood. Despite these minor errors, the confusion matrix demonstrates that the proposed model can effectively distinguish between multiple attack categories within Agriculture 4.0 networks.

6.4 Performance Discussion

The experimental results demonstrate that the proposed Random Forest model provides reliable multiclass intrusion detection for Agriculture 4.0 environments. The confusion matrix indicates high classification accuracy across most attack categories, while the feature importance analysis shows that only a limited number of network attributes contribute significantly to the prediction process. Also, the attack distribution shows that the model was tested with a range of data that includes both common and rare attack types. These results show that Random Forest is a choice for protecting agricultural IoT infrastructures because it can work with data that has many features, handle multiple classes, and deal with messy network traffic.

7. Future Research Directions

Future research should focus on developing more robust, efficient, and practical cybersecurity solutions for Agriculture 4.0.

Agriculture-Specific Datasets

Researchers should make datasets that show what really happens on agricultural networks and what kinds of attacks they face.

Explainable Artificial Intelligence

Using Explainable Artificial Intelligence can make things easier to understand and more transparent, which is a thing for Agricultural Internet of Things devices and Explainable Artificial Intelligence. Help people trust the decisions made by intrusion detection systems.

Federated Learning

Federated learning is a way for models to learn from each other without sharing all the information they have, which is really good for keeping things private and safe. Big places, with a lot of machines, make an amount of data, and that makes it really tough to go through all of it quickly and find the bad guys, like people who are trying to break in, and that is what federated learning and these systems are trying to do which is to find these bad people and stop them, and federated learning is helping with that.

Edge AI-Based Security

Deploying artificial intelligence models directly on Internet of Things devices can help with finding threats in real time while reducing the amount of communication needed.

Adaptive and Self-Learning IDS

Systems in the future should always update what they know and get used to cyber threats. Future research should focus on making cybersecurity solutions that are strong, efficient, and practical for Agriculture 4.0.

UAV and Smart Farm Security Integration

Combining drone security, sensor security, and network security into a unified framework can provide comprehensive protection for agricultural ecosystems.

8. Conclusion

The use of Agriculture 4.0 technologies has transformed modern agricultural practices. It has made farming more efficient by increasing the amount of food that can be produced and by making the whole process more efficient and friendly to the environment. With more machines and computers being connected to the internet, there is a bigger risk of cyberattacks that can disrupt agricultural operations and compromise connected systems and data. Artificial Intelligence and Machine Learning are valuable technologies for developing intelligent intrusion detection systems capable of identifying and responding to cyber threats. These systems are particularly useful for detecting complex and evolving threats that may be difficult to identify using conventional security approaches. Previous studies have demonstrated that Artificial Intelligence-based intrusion detection approaches can provide advantages over traditional security mechanisms in terms of detection accuracy, adaptability, and the ability to process large volumes of network data. They are more accurate can adapt to changing network conditions, and they can handle a large amount of data. There are still some problems that need to be solved. For example, the limited availability of agriculture-specific datasets, model interpretability, resource constraints, scalability, and the lack of real-world validation remain significant challenges. If these challenges can be addressed, the security and reliability of Agriculture 4.0 Agriculture 4.0 infrastructures can be further strengthened. Future developments in Explainable Artificial Intelligence, lightweight Machine Learning models, continuous learning, federated learning, and collaborative security mechanisms may play an important role in improving the robustness and adaptability of Agriculture 4.0 cybersecurity. New developments in Artificial Intelligence that can explain itself and in systems that can learn from each other will be very important for keeping Agriculture 4.0 safe from cyber threats.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

- [1] Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2022). *Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions*.
- [2] Keating, L. (2026). *AI-Based Detection of Cyber Intrusions in Food Supply Chains and Agricultural IoT Networks*.
- [3] Konstantinou, D., Stoyanov, S., Stoyanova, T., & Rafailov, R. (2025). *Securing the Internet of Things: The Role of Artificial Intelligence in Agricultural Cyber Defense*.
- [4] Mirmarghabi, M., Afshar, A., & Atrianfar, H. (2025). *Intrusion Detection System for Securing Agriculture 4.0 against DDoS Attacks using Deep Learning and Machine Learning Models*.
- [5] Mohamed, N. (2023). *Current Trends in AI and ML for Cybersecurity: A State-of-the-Art Survey*. *Cogent Engineering*, 10(2), 2272358.
- [6] Suneetha, C., Maloth, B., & Addepalli, L. (2026). *Cybersecurity Intrusion Detection in Industry 4.0 WSNs Using ML/DL*.

- [7] Khan, N., Ahmad, K., Al Tamimi, A., Alani, M. M., Bermak, A., & Khalil, I. (2024). *Explainable AI-Based Intrusion Detection System for Industry 5.0*.
- [8] Ojika, F. U., Owobu, W. O., Abieba, O. A., Esan, O. J., Ubamadu, B. C., & Daraojimba, A. I. (2024). *The Role of AI in Cybersecurity: A Cross-Industry Model for Integrating Machine Learning and Data Analysis for Improved Threat Detection*.
- [9] Diro, A. A., & Chilamkurti, N. (2018). Distributed Attack Detection Scheme Using Deep Learning Approach for IoT.
- [10] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics.