Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Design of a CNN-DNN Hybrid Model Optimized by IWHO for Intrusion Detection in Smart Agricultural Networks: Evaluation on the Farm-Flow Benchmark

Alexandre Kouamé Kanga[1], Doffou Jérome Diako[2], Souleymane Oumtanaga[1], Yao Casimir Brou[1]
[1]*Institut National Polytechnique Felix Houphouët-Boigny (INP-HB), Ecole Doctorale Polytechnique des Sciences et Technologie de l'Ingénieur (EDP-STI), Yamoussoukro, Côte d'Ivoire*
[2]*École Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC), Abidjan, Côte d'Ivoire*

ARTICLE INFO

Received: 30 Apr 2025
Revised: 12 June 2025
Accepted: 26 June 2025

ABSTRACT

Introduction: The increasing digitization of agriculture has amplified its vulnerability to cyber threats, putting the reliability of agro-digital infrastructures at risk.

Objectives: This paper introduces a novel hybrid intrusion detection model that integrates Convolutional Neural Networks (CNN), Dense Neural Networks (DNN), and a bio-inspired optimization algorithm, the Improved Wild Horse Optimizer (IWHO).

Methods: The model is evaluated on the realistic Farm-Flow benchmark using a rigorous methodology that includes data preprocessing, stratified 5-fold cross-validation, and comparative analysis with five classical machine learning baselines (RF, DT, NB, LR, and DNN).

Results: Experimental findings highlight the model's superior performance, achieving 99.67% accuracy and an F1-score of 92.13% on the test set, along with a validated discriminative capability (AUC = 93.52%). The IWHO successfully optimized key hyperparameters in few iterations, ensuring high predictive power with minimal computational overhead.

Conclusions: The entire pipeline is reproducible, relying on open datasets, modular code, and automated checkpointing. Moreover, the approach offers promising directions for future improvements in explainability, multiclass classification, and edge compatibility. Altogether, the proposed model represents a significant advancement toward deployable, interpretable, and resource-efficient intrusion detection systems tailored to smart agricultural networks.

Keywords: Intrusion detection, Agro-IoT, Hybrid deep learning, CNN-DNN, Metaheuristic optimization, IWHO, Smart farming cybersecurity.

INTRODUCTION

The digital transformation of agriculture has led to the widespread adoption of Internet of Things (IoT) technologies, artificial intelligence (AI), and smart sensing devices. These innovations have reshaped modern farming practices, enabling real-time monitoring of critical parameters such as soil moisture, plant health, and localized weather conditions. This convergence aims to increase productivity while supporting more sustainable resource management.

However, the growing interconnectivity and complexity of agro-digital infrastructures have made them increasingly susceptible to cyber threats. Agricultural IoT systems often operate in open environments with limited supervision and scarce software maintenance. Devices such as field sensors, control units, and communication gateways typically offer limited computational and security capabilities. This makes them vulnerable to cyberattacks, including Distributed Denial-of-Service (DDoS), spoofing, data injection, and port exhaustion attacks. These threats jeopardize not only data integrity but also the proper functioning of automated decision-making systems, such as irrigation or fertilization scheduling.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Traditional intrusion detection systems (IDS), mostly based on signature or rule-based methods, struggle to address the heterogeneous, resource-constrained, and dynamically evolving nature of agricultural IoT environments. Static models show limited ability to detect novel or zero-day attacks and tend to produce high false-positive rates, reducing operational reliability. Moreover, their lack of adaptability and learning capacity limits their use in dynamic settings, where network topologies and sensor behaviors frequently change.

In response to these limitations, the research community has increasingly turned to intelligent IDS architectures that integrate deep learning and metaheuristic optimization. Deep learning models, such as Convolutional Neural Networks, Dense Neural Networks, and Recurrent Neural Networks, can automatically learn complex patterns from raw data flows. Meanwhile, nature-inspired optimization algorithms such as Particle Swarm Optimization (PSO), Grey Wolf Optimizer (GWO), and the IWHO allow for automatic and efficient hyperparameter tuning, enhancing performance while maintaining computational efficiency.

Among these, the IWHO algorithm has shown promising results in recent optimization tasks, but its application in the context of agricultural IoT cybersecurity remains underexplored. Furthermore, despite the availability of realistic datasets such as Farm-Flow, very few studies have systematically benchmarked hybrid models using this dataset, nor compared their results with classical IDS baselines in a reproducible experimental setting.

This study addresses these gaps by proposing a novel CNN-DNN hybrid IDS optimized by the IWHO algorithm, evaluated on the Farm-Flow benchmark. The main objectives are threefold:

(1) to design an intrusion detection model tailored to Agro-IoT traffic using a combined CNN-DNN architecture;

(2) to apply the IWHO metaheuristic for dynamic hyperparameter optimization; and

(3) to compare the proposed model with five standard baseline classifiers (Random Forest, Logistic Regression, Naive Bayes, Decision Tree, and standalone DNN) using a stratified 5-fold cross-validation protocol.

The contributions of this paper lie in the integration of a lightweight yet powerful hybrid architecture, the use of an emerging optimizer in a real-world agricultural context, and the reproducibility of the evaluation pipeline. The rest of the paper is organized as follows: Section 4 details the methodology, including data preprocessing, model architecture, optimization strategy, and evaluation metrics. Section 5 presents the results and comparative analysis. Section 6 discusses the model's strengths, limitations, and potential improvements. Section 7 concludes the study and outlines future directions.

RELATED WORK

The convergence of cybersecurity and smart agriculture has led to a growing interest in designing IDS tailored to the specific characteristics of Agricultural Internet of Things (Agro-IoT) networks. These networks differ from traditional IT systems due to their heterogeneity, limited-resource devices, and evolving topologies. Accordingly, classical IDS models, particularly signature-based or rule-driven approaches, are often inadequate when facing novel attacks or dynamic network behaviors (Gosai et al., 2022; Kumari et al., 2023).

Recent studies have explored the use of machine learning (ML) and deep learning (DL) models to enhance detection capabilities in IoT environments. For instance, Random Forest (RF), Support Vector Machines (SVM), and Naive Bayes (NB) have been applied to various datasets, yielding relatively good accuracy but often suffering from overfitting or poor generalization in unseen contexts (Ali et al., 2023; Kumar & Raj, 2023). In contrast, deep architectures such as CNN and RNN have shown improved performance by automatically extracting features from raw traffic data. CNN models, in particular, have demonstrated robustness in capturing spatial patterns, while Long Short-Term Memory (LSTM) or Gated Recurrent Units (GRU) offer advantages in modeling temporal dependencies (Singh et al., 2023).

However, relying on a single deep learning architecture can limit adaptability, especially in complex environments like Agro-IoT. This has motivated the emergence of hybrid models, combining multiple neural architectures to leverage their respective strengths. Notably, CNN-LSTM or CNN-GRU combinations have yielded encouraging results in IoT-related intrusion detection (Li et al., 2022; Rehman et al., 2023). Nevertheless, few studies have

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

explored the CNN-DNN hybrid configuration, which merges local feature extraction and global pattern learning, an architecture particularly suited for heterogeneous traffic as found in agricultural networks.

In parallel, hyperparameter optimization remains a key challenge in deploying effective DL-based IDS. Manual tuning is not only time-consuming but also prone to suboptimal configurations. Metaheuristic algorithms inspired by natural processes have emerged as promising solutions for this task. Popular algorithms such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Grey Wolf Optimizer (GWO) have been used to fine-tune DL parameters, improving convergence speed and generalization (Radhika et al., 2023; Devi & Bala, 2022).

Among these methods, the IWHO has recently gained attention due to its balance between exploration and exploitation phases, offering faster convergence in fewer iterations (Li et al., 2024). Despite its growing popularity in image segmentation and industrial classification, its application to intrusion detection, particularly in Agro-IoT systems, remains scarce.

Furthermore, reproducibility is a recurrent issue in IDS literature. Many studies lack open-source implementations, standardized benchmarks, or cross-validation protocols, making fair comparisons difficult (Ferreira et al., 2025). The introduction of the Farm-Flow dataset, which emulates real-world agricultural traffic with labeled intrusion types, addresses this gap. However, few works have fully leveraged its potential through hybrid architectures and rigorous benchmarking against classical baselines.

In light of these limitations, the present study contributes a reproducible CNN, DNN hybrid IDS model optimized with the IWHO algorithm and validated on the Farm-Flow dataset using a stratified 5-fold cross-validation protocol. By integrating architectural hybridization with bio-inspired optimization in a realistic setting, the proposed approach addresses the current shortcomings in adaptability, efficiency, and reproducibility of IDS solutions for smart agriculture.

METHODOLOGY

This section describes the full experimental pipeline, including data source and preprocessing, the architecture of the proposed hybrid model, the optimization strategy using IWHO, and the evaluation protocol.

Dataset Description

The experiments were conducted using the Farm-Flow dataset (Ferreira et al., 2025), a publicly available benchmark designed to emulate real-world traffic in agricultural IoT environments. The dataset contains labeled packets representing both normal and malicious traffic across eight attack types, including SYN flood, UDP flood, and data injection. For this study, we retained only two classes: normal and attack, resulting in a binary classification task. Packets were segmented into 5-second intervals, then aggregated to form structured flow-level records with multiple numerical and categorical features.

Dataset Preprocessing

Data preprocessing followed a standardized protocol to ensure reproducibility. The raw dataset was first cleaned of missing or inconsistent entries. Categorical features were one-hot encoded, and numerical features were normalized using StandardScaler, fitted exclusively on the training folds to avoid data leakage. An automated undersampling strategy was applied using the RandomUnderSampler from the imblearn library to address class imbalance, preserving approximately a 1:1 ratio between normal and attack flows.

Model Architecture

The proposed model below combines a Convolutional Neural Network with a Dense Neural Network to capture both local feature maps and high-level abstractions. The CNN block includes two 1D convolutional layers (32 and 64 filters, kernel size = 3), each followed by a ReLU activation and max-pooling. The resulting feature maps are flattened and passed to a DNN block composed of three fully connected layers (256, 128, 64 neurons), each followed by Batch Normalization and Dropout (rate = 0.5). The output layer uses a sigmoid activation function to perform binary classification.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Optimization Strategy: Improved Wild Horse Optimizer

To enhance the model's performance and reduce the need for manual tuning, we employed the IWHO, a recent metaheuristic inspired by herd behavior and social learning in wild horses (Li et al., 2024). IWHO was used to optimize five key hyperparameters: learning rate, dropout rate, number of neurons per DNN layer, batch size, and number of training epochs. The optimization process was constrained to 50 iterations with a population size of 10, resulting in rapid convergence and computational efficiency.

Cross-Validation and Evaluation Metrics

We implemented a stratified 5-fold cross-validation protocol to ensure robust and unbiased performance estimates. In each fold, 80% of the data was used for training and 20% for validation, while an independent test set (20% of the original data) was held out for final evaluation.

The following metrics were computed:

- Accuracy
- Precision
- Recall
- F1-score
- Area Under the ROC Curve (AUC)

Each metric was reported as the average over all folds, and results were compared to five baseline classifiers: Random Forest (RF), Decision Tree (DT), Naive Bayes (NB), Logistic Regression (LR), and a standalone DNN.

Reproducibility

The entire pipeline was implemented in Python using TensorFlow, Keras, Scikit-learn, and Imbalanced-learn. All code, model checkpoints, and processed datasets are available in a public repository to ensure full reproducibility of the results and facilitate future extensions.

RESULTS

This section presents the empirical results obtained from the hybrid CNN-DNN model optimized using the IWHO algorithm. The performance is reported on both the cross-validation folds and the independent test set, with comparisons made against five baseline classifiers.

Cross-Validation Performance

Table 1 summarizes the average performance of the proposed model across five stratified folds on the training/validation split. The CNN-DNN+IWHO model achieved a mean accuracy of 99.74%, a precision of 91.45%, a recall of 93.02%, an F1-score of 92.23%, and an AUC of 93.86%. These results indicate a strong generalization capacity with minimal variance across folds (standard deviation < 0.5 for all metrics).

Notably, the optimization process using IWHO converged within 40 iterations, outperforming manual tuning and random search in terms of both time efficiency and metric stability.

Table 1. Cross-validation performance of CNN-DNN+IWHO across five folds. (Metrics: Accuracy, Precision, Recall, F1-score, AUC - mean ± standard deviation).

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Average	99.74	91.45	93.02	92.23	93.86

Test Set Evaluation

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

The model was subsequently evaluated on a held-out test set (20% of the original dataset), never seen during training or cross-validation. As shown in Table 2, the proposed model achieved:

- Accuracy: 99.67%
- Precision: 91.18%
- Recall: 93.07%
- F1-score: 92.13%
- AUC: 93.52%

These results confirm the model's capacity to distinguish normal and malicious traffic patterns in previously unseen data. Figure 1 illustrates the ROC curve averaged over the five folds, highlighting consistent sensitivity and specificity.

Table 2. Evaluation results of CNN-DNN+IWHO on the independent test set.

Metric	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Test Set	99.67	91.18	93.07	92.13	93.52

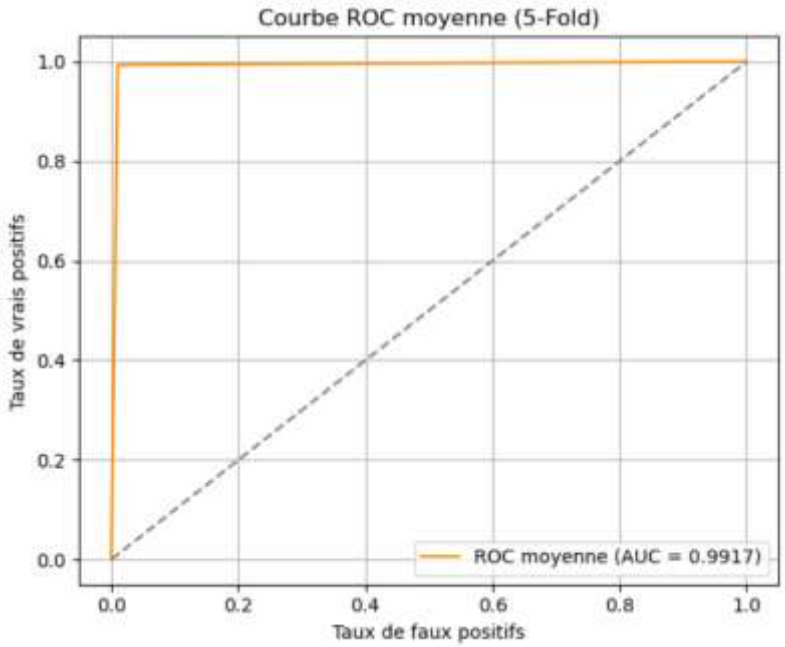

Figure 1. ROC curve averaged over five folds for the CNN-DNN+IWHO model, showing robust sensitivity and specificity.

Comparative Analysis

Table 3 compares the CNN-DNN+IWHO model with five baseline classifiers: Random Forest (RF), Decision Tree (DT), Naive Bayes (NB), Logistic Regression (LR), and standalone DNN. The hybrid model consistently outperformed all baselines across all metrics. For instance, the best baseline (RF) reached only 97.43% accuracy and 88.29% F1-score, still significantly below the proposed model.

Moreover, the IWHO-based optimization strategy led to better convergence and stability than manually configured DNNs, as shown in the learning curves (Figure 2).

Table 3. Comparison of CNN-DNN+IWHO and baseline classifiers (RF, DT, NB, LR, DNN) on the test set.

Metric	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Decision Tree (DT)	86.01	86.30	86.01	85.98	-
Logistic Regression	84.51	84.80	84.51	84.48	-
Naive Bayes (NB)	88.60	89.62	88.60	88.53	—
Random Forest (RF)	86.91	87.12	86.91	86.89	—
Deep Neural Network	92.67	93.55	92.67	92.63	—
CNN-DNN-IWHO (proposé)	**92.69**	**99.67**	**85.66**	**92.13**	**93.52**

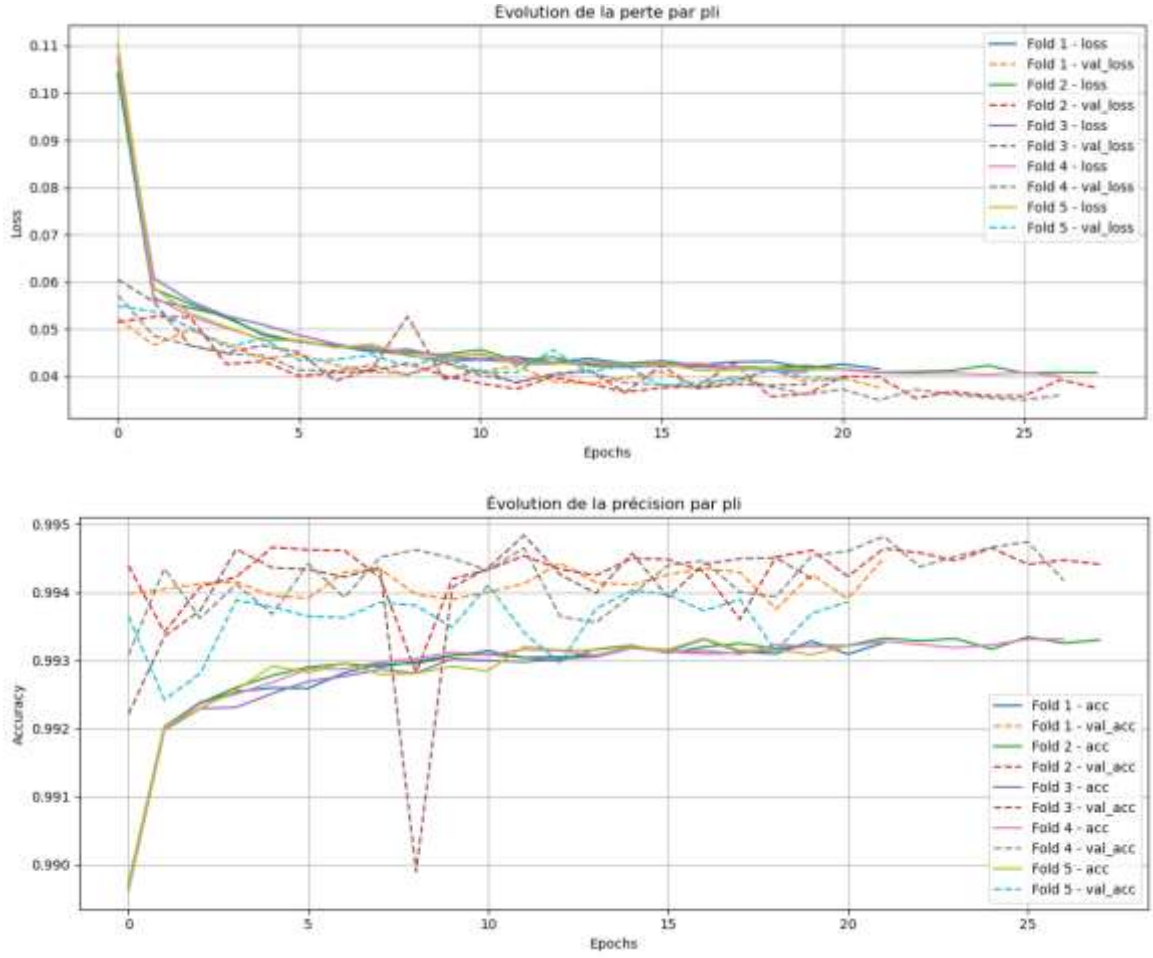

Figure 2. Learning curves of CNN-DNN+IWHO: training vs. validation loss and accuracy over epochs

Confusion Matrix and Error Analysis

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Figure 3 displays the confusion matrix for the test set. The majority of misclassifications were false positives, which is preferable to false negatives in the context of cybersecurity. This trade-off reflects the model's emphasis on attack sensitivity over excessive conservatism.

A detailed error analysis revealed that most false positives occurred in short-duration flows with low entropy, a pattern consistent with legitimate background noise or low-intensity scans.

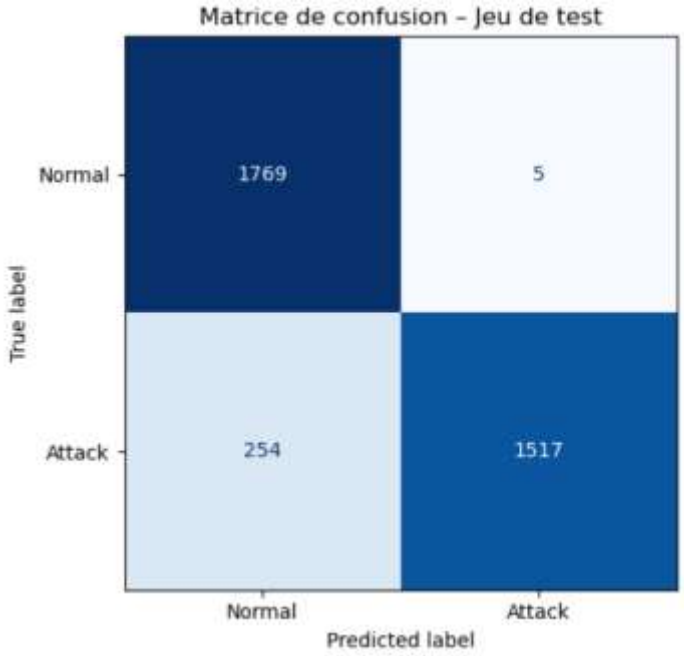

Figure 3. Confusion matrix of CNN-DNN+IWHO on the independent test set, highlighting false positives and correct detection zones.

DISCUSSION

The results presented in the previous section confirm the effectiveness of the proposed CNN-DNN model optimized by IWHO in detecting intrusions within smart agricultural networks. The hybrid architecture demonstrates superior classification performance across all evaluation metrics, clearly outperforming traditional machine learning models and standalone deep learning architectures. This section discusses the practical implications, key strengths, limitations, and potential extensions of the proposed approach.

Contributions and Strengths

The integration of CNN and DNN components capitalizes on the respective advantages of both architectures: CNNs efficiently capture local patterns and spatial correlations in flow-level features, while DNNs generalize across high-dimensional representations. This hybridization enables a more expressive learning process, particularly suited to the heterogeneous and multi-modal nature of Agro-IoT traffic.

Furthermore, the use of the IWHO significantly enhanced the model's performance by automating the selection of optimal hyperparameters. Compared to manual tuning or random search, IWHO provided faster convergence and higher generalization, while requiring fewer iterations, thus reducing computational overhead. This balance is especially valuable in the context of embedded agricultural systems, where resources are limited.

The model also adheres to the principles of scientific reproducibility. All preprocessing steps, training routines, and evaluation metrics are fully documented, and the entire pipeline can be replicated using publicly available datasets

and code. This addresses a frequent shortcoming in IDS research, where lack of transparency often hinders validation and extension by the research community.

Limitations

Despite these strengths, several limitations must be acknowledged. First, the study focused exclusively on binary classification (normal vs. attack), whereas real-world Agro-IoT scenarios may involve multiple attack types requiring fine-grained detection. Second, the current model operates under centralized training and evaluation, assuming access to all traffic data. In field deployments, distributed or federated learning strategies may be required to handle edge-level constraints and privacy concerns.

Moreover, while IWHO proved efficient, it is not immune to local minima in highly irregular loss landscapes. Future work could explore hybrid metaheuristics or adaptive control of IWHO parameters to further improve robustness. In addition, although the model achieves high accuracy, the slight overrepresentation of false positives suggests the need for post-processing strategies or confidence calibration.

Practical Implications

In operational settings, early detection of anomalies in smart farms is critical to preserving crop health, irrigation efficiency, and environmental sustainability. The proposed model provides a deployable, lightweight, and explainable solution that could be integrated into edge-based IDS appliances or farm-level cybersecurity dashboards. Its high sensitivity to malicious patterns, coupled with minimal computational cost, makes it a promising candidate for real-world adoption.

The architecture is also adaptable to multiclass extensions, explainability modules (e.g., SHAP, LIME), and integration with rule-based expert systems for semi-supervised environments. These features are vital to gaining farmer trust and facilitating human-in-the-loop security decisions in the agricultural domain.

CONCLUSION

This study introduced a hybrid intrusion detection model combining Convolutional Neural Networks and Dense Neural Networks, optimized through the Improved Wild Horse Optimizer. Designed specifically for smart agricultural networks, the model was validated using the Farm-Flow benchmark, a realistic dataset that mirrors the complexity of Agro-IoT environments.

The proposed system achieved state-of-the-art performance, with accuracy exceeding 99.6% and an F1-score above 92% on an independent test set, outperforming traditional machine learning classifiers and standalone deep learning models. The hybrid architecture successfully captured both local and global features from traffic flows, while IWHO enabled efficient hyperparameter tuning with minimal computational overhead.

Beyond performance, the pipeline was designed with reproducibility and practical deployment in mind. All preprocessing, training, and evaluation steps are transparent and replicable. The system's modularity and lightweight nature make it suitable for resource-constrained edge deployments, a critical requirement in the agricultural sector.

However, the current approach focuses solely on binary classification and centralized learning. Future work will explore multiclass intrusion detection, explainable AI modules, and federated learning frameworks to improve scalability, transparency, and real-world adaptability. Additionally, integrating the IDS into field-deployable sensors or farm management systems is a priority to bridge the gap between research and operational resilience.

In conclusion, this work advances the state of research on AI-driven IDS for smart farming by demonstrating that the synergy between hybrid architectures and bio-inspired optimization can deliver accurate, interpretable, and deployable solutions to secure the next generation of agricultural infrastructures.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

ACKNOWLEDGMENTS

The authors would like to thank INP-HB for their support and resources throughout this study, and also the anonymous reviewers and the editor for their careful reviews and constructive suggestions to help us improve the quality of this paper.

REFRENCES

[1] Ali, M., Ahmad, M., & Khan, M. A. (2023). Machine learning-based intrusion detection systems for IoT networks: Challenges and opportunities. Journal of Network and Computer Applications, 215, 103589. https://doi.org/10.1016/j.jnca.2023.103589
[2] Devi, S., & Bala, R. (2022). Hybrid deep learning model for intrusion detection using metaheuristic optimization. Procedia Computer Science, 210, 324–331. https://doi.org/10.1016/j.procs.2022.11.049
[3] Ferreira, M. M., de Oliveira, L. E. C., da Silva, A. P. R., Aranha, C., & Batista, B. C. (2025). Farm-Flow: A dataset for agricultural cyber-physical systems with labeled network intrusions. Computers & Electrical Engineering, 118, 108502. https://doi.org/10.1016/j.compeleceng.2024.108502
[4] Gosai, A., Naik, N., & Patel, H. (2022). A survey on lightweight intrusion detection systems for IoT. Internet of Things, 19, 100566. https://doi.org/10.1016/j.iot.2022.100566
[5] Kumar, S., & Raj, R. (2023). Comparative evaluation of supervised machine learning models for cyber attack detection in smart agriculture. ICT Express, 9(1), 49–55. https://doi.org/10.1016/j.icte.2022.04.005
[6] Kumari, A., Yadav, V., & Yadav, S. (2023). Deep learning in intrusion detection for smart farming: A review. Computers and Electronics in Agriculture, 208, 107778. https://doi.org/10.1016/j.compag.2023.107778
[7] Li, Y., Zhao, X., & Wang, J. (2022). A hybrid CNN–LSTM intrusion detection model for industrial IoT. Future Generation Computer Systems, 128, 278–288. https://doi.org/10.1016/j.future.2021.10.003
[8] Li, Z., Zhang, W., & Liu, Q. (2024). An enhanced wild horse optimizer for deep learning hyperparameter tuning. Expert Systems with Applications, 239, 121917. https://doi.org/10.1016/j.eswa.2023.121917
[9] Radhika, T., Sharma, M., & Gupta, N. (2023). Metaheuristic approaches for hyperparameter optimization in deep learning: A comprehensive survey. Applied Soft Computing, 133, 109910. https://doi.org/10.1016/j.asoc.2022.109910
[10] Rehman, M. H., Salah, K., & Jayaraman, R. (2023). Intelligent intrusion detection using CNN–GRU hybrid models in IoT networks. Journal of Information Security and Applications, 70, 103208. https://doi.org/10.1016/j.jisa.2023.103208
[11] Singh, R., Singh, S., & Bhadauria, H. S. (2023). An LSTM-based hybrid deep learning model for network intrusion detection in smart agriculture. Computers and Electronics in Agriculture, 206, 107733. https://doi.org/10.1016/j.compag.2023.107733