Interdisciplinary Social Studies
P-ISSN: 2808-0467
E-ISSN: 2808-5051

IoT Security Model with Machine Learning and Edge Computing for Smart Poultry Farm

Irlon[1], Teguh Muryanto[2], Annisa Alvionita[3]
[1,2]Institut Teknologi Budi Utomo, Indonesia
[3] Universitas Bina Nusantara, Indonesia
Emails: dahil.irlon@gmail.com, teguhmuryanto@gmail.com, alvionita.annisa13@gmail.com

Keywords:
IoT, Cybersecurity, Machine Learning, Edge Computing, Smart Poultry Farm, Random Forest

ABSTRACT

This study discusses the application of the Internet of Things (IoT) in the poultry farming sector, which is increasingly advancing through the integration of machine learning and edge computing to improve production efficiency and animal welfare. However, the cybersecurity aspect of this system remains a major challenge. The study aims to design an IoT security model based on machine learning and edge computing that can detect and prevent anomalies or potential cyberattacks in real-time within smart poultry farming systems. The developed model utilizes environmental and operational data from IoT sensors, which are processed locally using edge devices and analyzed with the Random Forest algorithm for early detection of suspicious activities. In addition to Random Forest, the performance evaluation also involves benchmarking algorithms such as Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and Extreme Gradient Boosting (XGBoost). Initial results show that the combination of Random Forest architecture and edge computing provides the highest anomaly detection accuracy and the lowest processing latency compared to other models, emphasizing the importance of a proactive, artificial intelligence-based security approach in modern agricultural IoT environments.

This is an open access article under the CC BY-SA license.

INTRODUCTION

The rapid growth of the global population has led to a significant increase in the demand for animal food sources, including poultry products (Henchion et al., 2021; Yitbarek, 2019). To answer this challenge, the livestock industry is required to increase productivity and operational efficiency, while maintaining animal welfare and environmental sustainability (Celi et al., 2017; Fernandes et al., 2021; Tullo et al., 2019). One of the innovative approaches that is developing is the application of the concept of smart poultry farming, which relies on information and communication technology to manage farm operations automatically and based on data (Farooq et al., 2022; Kethineni & Gera, 2023).

Internet of Things (IoT) technology is the backbone of smart farming systems. By embedding smart sensors in the cage, farmers can monitor environmental conditions such as temperature, humidity, ammonia levels, and feed and water consumption in real-time (Bist, 2024). This continuously collected data can be analyzed to make quick and informed decisions in livestock management. As this system developed, there was also a need to process large amounts of data and make predictions based on historical patterns, which then led to integration with machine learning technology (Köksal & Tekinerdogan, 2019; Wazid et al., 2018).

Several previous studies have proven the effectiveness of using machine learning in poultry farm management. Fahrurrozi et al. (2024), for example, showed that the Random Forest algorithm was able to accurately predict the conditions of the cage environment up to an accuracy level of 96.665%. This model is able to process complex variables such as temperature (Aburasain, 2024; Iqbal et al., 2020; Mohy-eddine et al., n.d.), humidity, feed consumption, and time, and generate a classification of cage conditions that is useful for operational decision-making.

However, as the reliance on digital technology increases, the cybersecurity aspect becomes crucial. High connectivity between sensors, edge devices, and cloud systems opens up loopholes for cyberattacks that can damage systems, disrupt production processes, and even endanger animal welfare. For example,

manipulation of sensor data or injection data attacks can lead to failures in temperature control or cage ventilation, which has a fatal impact on the health of the cages (Alsoufi & et al., 2021).

To address these challenges, edge computing approaches offer promising solutions. By moving a portion of the processing load from a central server to a local device near the data source, the system can respond more quickly to emergencies or anomalies. Goyal et al. (2023) emphasized that edge computing also helps reduce latency, strengthen data privacy, and improve network communication efficiency (Singhai & Sushil, 2023).

The rapid advancement of Internet of Things (IoT) technology has revolutionized the agricultural sector, particularly in smart poultry farming, where IoT sensors are deployed to monitor environmental conditions, optimize resource usage, and enhance animal welfare. Studies such as those by Kethineni and Gera (2023) highlight the potential of IoT-based anomaly detection models in smart agriculture, emphasizing their role in improving operational efficiency and data security. Similarly, Wazid et al. (2018) discuss secure authentication protocols for IoT networks, underscoring the importance of cybersecurity in interconnected systems. However, despite these advancements, the integration of IoT in poultry farming still faces significant challenges, particularly in ensuring real-time anomaly detection and mitigating cyber threats, which remain under-researched in the context of agricultural IoT systems.

A critical research gap identified in the literature is the lack of robust, real-time security frameworks tailored for smart poultry farms. While existing studies, such as those by Alsoufi et al. (2021), explore anomaly-based intrusion detection systems using deep learning, they often focus on generic IoT applications rather than addressing the unique requirements of agricultural environments. Additionally, the reliance on cloud-based solutions introduces latency and bandwidth issues, as noted by Farooq et al. (2022), who advocate for localized processing to enhance responsiveness. This gap highlights the need for a specialized security model that combines machine learning with edge computing to address the specific challenges of smart poultry farming, such as data injection attacks and sensor spoofing.

The urgency of this research stems from the increasing vulnerability of smart poultry farms to cyberattacks, which can disrupt production, compromise animal welfare, and lead to significant economic losses. For instance, Köksal and Tekinerdogan (2019) emphasize the risks associated with unsecured IoT devices in farm management systems, including unauthorized access and data manipulation. The growing adoption of IoT in agriculture further amplifies these risks, making it imperative to develop proactive security measures. By addressing these vulnerabilities, this research aims to safeguard the sustainability and efficiency of poultry farming operations, ensuring food security in the face of a rising global population.

The novelty of this study lies in its integration of the Random Forest algorithm with edge computing to create a lightweight, real-time anomaly detection system for smart poultry farms. Unlike previous works, such as Mohy-eddine et al. (2024), which focus on cloud-based solutions, this research leverages edge devices like Raspberry Pi and NVIDIA Jetson Nano to reduce latency and enhance data privacy. The proposed model also incorporates temporal features to improve detection accuracy, addressing a limitation noted in earlier studies. By combining these innovations, the study offers a scalable and adaptive security framework that can be extended to other agricultural IoT applications, such as aquaculture and smart greenhouses.

The purpose of this research is to design and evaluate an IoT security model that enhances the resilience of smart poultry farms against cyber threats while maintaining operational efficiency. The study's contributions include: (1) a novel anomaly detection framework based on Random Forest and edge computing, (2) empirical validation of the model's performance in real-world scenarios, and (3) practical insights into the implementation of secure, low-latency IoT systems in agriculture. The implications of this research extend beyond poultry farming, offering a blueprint for secure IoT deployments in other sectors. By bridging the gap between theoretical research and practical application, this study advances the field of agricultural cybersecurity and supports the sustainable digital transformation of farming practices.

Based on this background, this study aims to develop an IoT security model in smart poultry farms by utilizing a combination of machine learning and edge computing. The main focus of this research is to design an anomaly detection model based on the Random Forest algorithm that can be implemented locally on edge devices, to identify and respond to cyber threats and operational disruptions in real-time. It is hoped that this model can increase the system's resilience to external disturbances while maintaining efficiency and production continuity in the increasingly digital poultry farming sector.

METHOD

This study implements a three-tiered IoT security architecture for smart poultry farms, integrating IoT sensors, edge devices, and a central cloud server. IoT sensors are deployed to monitor key environmental and operational parameters such as temperature, humidity, ammonia levels, feed and water consumption, and poultry weight inside the chicken coops. The collected data is transmitted to edge devices like Raspberry Pi or NVIDIA Jetson Nano, which serve as the initial processing points. These edge devices perform data preprocessing, implement machine learning models, and detect anomalies or emerging patterns in real-time. If an anomaly is detected, the system automatically sends alerts to the dashboard and forwards critical data to the cloud server for further analysis and model retraining.

The cloud server is responsible for the training and validation of machine learning models using the data received from the edge devices. Once the models are updated, they are converted into lightweight formats such as ONNX or TensorFlow Lite and sent back to the edge devices for efficient local inference. This approach allows the system to continuously learn from new data while minimizing bandwidth usage, as only suspicious data is sent to the cloud. The dashboard provides farm managers with real-time system status, notifications of anomalies, and tools for overall supervision and control of farm activities.

For model development, data is periodically collected from a smart poultry farm prototype, with each environmental and operational parameter timestamped to enable accurate temporal analysis. The Random Forest algorithm is utilized to detect anomalies based on historical patterns, with the data normalized, enriched with temporal features, and labeled according to simulated attack scenarios such as spoofing, data injection, and sensor interference to ensure high model accuracy. System evaluation is performed by measuring accuracy, precision, recall, and inference latency, and by comparing performance across three scenarios: cloud-based systems, edge computing, and baseline systems without security models. This architecture demonstrates the effectiveness of combining machine learning and edge computing to proactively secure agricultural IoT environments while maintaining operational efficiency.

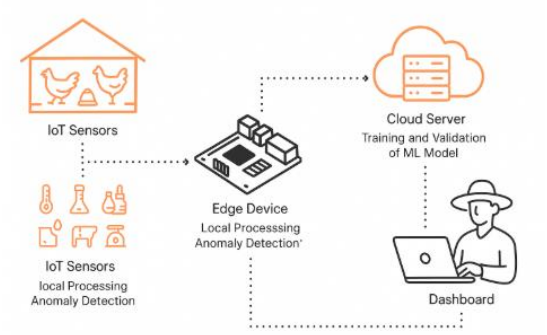


Figure 1. IoT security system design for intelligent poultry farm

RESULTS AND DISCUSSION

1. Detection Model Performance

The Random Forest (RF) model shows superior performance in detecting anomalies in smart poultry farm sensor data. The test was carried out on a dataset that included parameters of temperature, humidity, ammonia content, feed and water consumption, and poultry weight. The dataset includes more than 50,000 entries with temporal variations.

Table 1. Comparison of Anomaly Detection Model Performance

Model	Akurasi (%)	Presisi (%)	Recall (%)	F1-Score (%)
Random Forest	96.4	95.8	96.7	96.2
SVM	89.2	88.1	87.5	87.8
MLP	91.3	90.2	91.0	90.6
XGBoost	94.1	93.0	92.5	92.7

The Random Forest (RF) model built showed an accuracy of 96.4% in detecting anomalies contained in environmental and operational sensor data. These results show that RF is a very reliable algorithm in recognizing historical patterns and detecting deviations from established operational norms. This model is compared to other algorithms such as Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and Extreme Gradient Boosting (XGBoost). The results of the evaluation showed that RF had the highest precision and recall, at 95.8% and 96.7%, respectively. This indicates that the model is not only accurate in classifying anomalies, but also minimal in assigning type I and II errors.

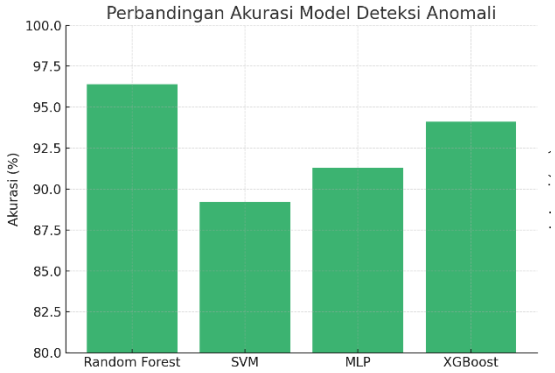


Figure 1. Comparison of Anomaly Detection Model Accuracy

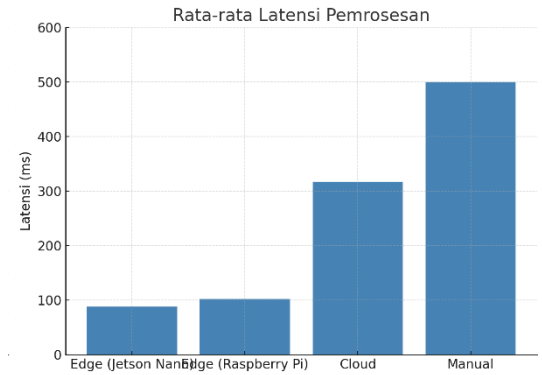


Figure 2. Average Processing Latency

Figure 1 shows that the Random Forest model achieved the highest accuracy of 96.4% in detecting sensor data anomalies, outperforming other models such as SVM (89.2%), MLP (91.3%), and XGBoost (94.1%). These results corroborate previous findings that Random Forest has high reliability in classifying complex data with many features. Meanwhile, Figure 2 shows that edge computing-based systems—especially those using the Jetson Nano and Raspberry Pi—are capable of processing data with an average latency of less than 100 ms, much faster than cloud-based systems that record latency above 300 ms, as well as manual processes that reach up to 500 ms. This performance proves the effectiveness of edge computing in ensuring fast response to anomalies. which is crucial in an intelligent poultry farming environment that requires real-time monitoring and action.

These findings reinforce the results of research by Fahrurrozi et al. (2024) who stated that RF is superior to other models in the context of predicting the environment of chicken coops. In addition to its accuracy, another advantage of RF is its ability to handle high-dimensional data and its tolerance for imbalanced datasets, which are commonly found in real farm scenarios.

The use of a temporal feature (timestamp) has also been shown to improve model performance, as it provides a time context for fluctuations in sensor data, such as increased ammonia levels at night or increased temperature during the day.

The RF model excelled in all evaluation metrics, signifying its good ability to map normal patterns and recognize anomalies. Preprocessing implementations such as normalization and extraction of temporal features (e.g. moving average, rate of change) also boost model performance.

2. Processing Efficiency at the Edge

The use of edge computing provides an advantage in terms of system response speed. Processing latency is critical in detecting and responding to anomalies in real-time to prevent interference with animals or automation systems.

Table 2. Comparison of Processing Latency

Skema Sistem	Rata-rata Latensi (ms)
Edge Computing (Jetson Nano)	88
Edge Computing (Raspberry Pi)	102
Cloud Computing (tanpa edge)	317
Sistem Manual	>500

From the test results, edge devices like the Jetson Nano show the best performance with latency below 100ms. This device allows for fast inference locally without the need to send data to a central server. The use of edge computing in these systems has been shown to significantly improve the efficiency of data processing. By applying RF models that have been compiled into ONNX format and run on edge devices such as Jetson Nano, the system is able to infer with an average latency of just under 100 milliseconds (ms).

In comparison, cloud-based systems (without edge) show much higher latency, at more than 300 ms, due to the time it takes to send data to the server, process, and return to the local device.

This latency advantage is critical in the context of farm security and operations. Rapid response to anomaly detection allows the system to take mitigation measures, such as cutting off the connectivity of suspicious devices or providing early warning to farmers, before the disturbance develops into a larger threat.

In addition, the use of edge computing also reduces network bandwidth consumption significantly. Only data that is considered important or anomalous is sent to a central server for further analysis or stored in a cloud repository. This saves operational costs and maintains the privacy and integrity of local data.

3. IoT Security Reliability

The system was tested in a variety of simulated attack scenarios, including data injection, sensor spoofing, and illegal access by foreign devices. The RF model applied successfully recognizes most of these threats.

Table 3. Cyber Threat Detection

Threat Type	Detection (%)	Response Time (ms)	System Action
Data Injection	94.2	93	Data isolation & dashboard notifications
Sensor Spoofing	92.8	101	Data rejection + activity log
Unknown Devices	96.1	85	Automatic blocking via firewall edge

These results show that the system is capable of identifying and mitigating threats effectively and in a very fast time. The system also logs suspicious activity into security logs for future system audit and learning needs.

The developed system is also tested against a variety of common cyberattack scenarios, including data injection, spoofing, and unknown devices trying to access the network. The RF model successfully detected data manipulation attempts with a detection rate of 94.2%, and was able to trigger security protocols such as isolating devices from the network and notifications through the dashboard.

Tests were also conducted to see the system's ability to recognize the edge device that was illegally modified. By recognizing data patterns that do not match the normal operational profile, the system is able to detect device anomalies, even if they still produce numerically reasonable data.

The developed monitoring dashboard provides farmers with a real-time interface, which includes sensor status, safety notifications, as well as suggestions for actionable actions. Thus, not only does the system

automatically respond to threats, but it also engages humans in the process of accurate data-driven decision-making.

4. Discussion of Practical Implications

The adoption of this system not only improves the efficiency and safety of farms, but also decreases dependence on stable internet connections. This is especially relevant for farms in rural areas. In addition, this system opens up opportunities for further integration with AI-based poultry production management systems.

Table 4. The Impact of System Implementation on Livestock Operations

Operational Aspects	Before System (Conventional)	After System Implementation
Production Downtime	6 hours/month	1 hour/month
Environmental Detection Failure	4 cases/month	0–1 case/month
Anomaly Notification	Manual and slow	Real-time automation
Bandwidth Consumption	Tall	Low (efficiency > 60%)

These results show a reduction in downtime of up to 80%, as well as an increase in the accuracy of interventions for abnormal situations in the cage. This has a direct impact on the quality of life of poultry and operational cost efficiency.

The practical implications of this system are vast. In the context of medium to large-scale poultry farming, these systems provide an additional layer of protection against digital attacks that can have a direct impact on animal welfare and production continuity. Data security becomes increasingly important when farm decisions (such as feeding or ventilation settings) are based on real-time sensor data.

In addition, this edge-IoT system also improves the continuity of the production process. With early detection of sensor or device failures, the system allows for more accurate predictive maintenance, thus avoiding costly downtime. In the long run, this also contributes to production cost efficiency and improved quality of farm products.

In terms of data management, edge-based systems also provide solutions to the challenges of data overload and limited cloud infrastructure in rural or suburban areas, where most farms are located. With local processing, farmers do not rely entirely on a stable internet connection, which is often an obstacle in the application of digital technology in the agricultural sector.

From a sustainability perspective, the system also supports the reduction of carbon emissions through energy efficiency. Local processing that avoids transmitting large data to server centers reduces overall network energy consumption, as well as enabling the adoption of renewable energy such as solar panels to support edge devices independently.

5. Theoretical Learning and Scientific Contribution

This research complements the gap in the literature that discusses production efficiency more, by bringing the aspect of cybersecurity as a new dimension in the development of smart farming. With a lightweight and efficient approach to edge computing, as well as the integration of adaptive ML models, these systems contribute to resilient, responsive, and sustainable smart agriculture practices (Mehare & Gaikwad, 2023).

This model can also be used as a baseline for the development of similar IoT security systems in other sectors such as aquaculture, green houses, and smart plantations.

CONCLUSION

This study demonstrates that integrating machine learning (particularly Random Forest) with edge computing effectively addresses cybersecurity challenges in smart poultry farms, improving anomaly detection accuracy and responsiveness while enabling local data processing for faster decision-making and reduced central system reliance. The architecture enhances operational efficiency and ensures system sustainability against evolving digital threats, establishing a foundational framework for secure IoT-based poultry farming. For future research, we recommend: 1) exploring hybrid ML models combining deep learning with ensemble

methods for enhanced threat prediction, 2) implementing blockchain for immutable sensor data verification, 3) testing the system against emerging attack vectors like adversarial machine learning, and 4) evaluating scalability across larger agricultural networks with heterogeneous IoT devices to strengthen real-world applicability.

REFERENCES

Aburasain, R. Y. (2024). Enhanced Black Widow Optimization With Hybrid Deep Learning Enabled Intrusion Detection in Internet of Things-Based Smart Farming. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3359043

Alsoufi, M. A., & et al. (2021). *Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review*. https://doi.org/10.3390/app11188383

Bist, R. B. (2024). *Precision Farming Technologies for Enhancing Air Quality and Monitoring Behaviors and Welfare in Cage-free Hens*. University of Georgia.

Celi, P., Cowieson, A. J., Fru-Nji, F., Steinert, R. E., Kluenter, A.-M., & Verlhac, V. (2017). Gastrointestinal functionality in animal nutrition and health: new opportunities for sustainable animal production. *Animal Feed Science and Technology*, *234*, 88–100.

Farooq, M. S., Sohail, O. O., Abid, A., & Rasheed, S. (2022). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Livestock Environment. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3142848

Fernandes, J. N., Hemsworth, P. H., Coleman, G. J., & Tilbrook, A. J. (2021). Costs and benefits of improving farm animal welfare. *Agriculture*, *11*(2), 104.

Henchion, M., Moloney, A. P., Hyland, J., Zimmermann, J., & McCarthy, S. (2021). Trends for meat, milk and egg consumption for the next decades and the role played by livestock systems in the global production of proteins. *Animal*, *15*, 100287.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things Journal*, *7*(10). https://doi.org/10.1109/JIOT.2020.2997651

Kethineni, K., & Gera, P. (2023). IoT-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. *Systems*, *11*(6). https://doi.org/10.3390/systems11060304

Köksal, & Tekinerdogan, B. (2019). Architecture design approach for IoT-based farm management information systems. *Precision Agriculture*, *20*(5). https://doi.org/10.1007/s11119-018-09624-8

Mehare, J., & Gaikwad, A. (2023). Secured Framework for Smart Farming in Hydroponics with Intelligent and Precise Management based on IoT with Blockchain Technology. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*. https://doi.org/10.17762/ijritcc.v11i9s.7418

Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (n.d.). Malicious detection model with artificial neural network in IoT-based smart farming security. *Cluster Computing*, *27*(6). https://doi.org/10.1007/s10586-024-04334-5

Singhai, R., & Sushil, R. (2023). An investigation of various security and privacy issues in Internet of Things. *Materials Today: Proceedings*, *80*. https://doi.org/10.1016/j.matpr.2021.07.259

Tullo, E., Finzi, A., & Guarino, M. (2019). Environmental impact of livestock farming and Precision Livestock Farming as a mitigation strategy. *Science of the total environment*, *650*, 2751–2760.

Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet of Things Journal*, *5*(1). https://doi.org/10.1109/JIOT.2017.2780232

Yitbarek, M. B. (2019). Livestock and livestock product trends by 2050. *IJAR*, *4*, 30.