Vol. 06, No. SI♣, pp. 15 –24 (2025)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

Real-Time Secure Cloud Transmission Framework for Agricultural Surveillance Using YOLOv5, AES-256, and HMAC-SHA256

Himanshu[1], Harwant Singh Arri[2], Ravi Kumar[3], Vishal Kumar Singh[4], Aman Deep[5] and Akash Badhan[*6]

[1,2,3,5,6] *School of Computer Science and Engineering, Lovely Professional University, India, (himanshuy69486@gmail.com, hsarri@gmail.com, ravi8507cpr@gmail.com, amanpal84@gmail.com)*
[6]*Department of IT, National Institute of Technology, Jalandhar, Punjab, India, er.akashbadhan@gmail.com*
[4]*School of Computer Science and Engineering, Parul University, Vadodara, India, vishalkumarsingh162@gmail.com*

**Corresponding author: er.akashbadhan@gmail.com*

Abstract

The agricultural surveillance systems produce unending floods of delicate visual information that needs to be sent safely to cloud-based infrastructures to be subjected to real-time interpretation and decision-making processes. The current paper introduces a new real-time, lossless, and secure edge-to-cloud transmission model which combines YOLOv5-based event detection, AES-256 symmetric encryption, and HMAC-SHA256 integrity checks and verifies into a single system. The system identifies critical events and encrypts locally and sends only the authenticated data to the cloud thus maintaining confidentiality, integrity and availability. It was evaluated on a custom dataset of 8,000 agricultural images with an average encryption time of 0.17 s/image, decryption time of 0.16 s/image and SSIM of 1.00, which validates the lossless image quality. YOLOv5 model attained 98.5 percent mean average precision (mAP @0.5), which guarantees correct detection prior to encryption. Comparison shows that the suggested approach is faster, more scalable, and more robust in comparison with the existing machine learning and standalone encryption systems. The model provides a scalable architecture of safe, smart farming surveillance, which will form the foundation of future updates pertaining to post-quantum encryption and federated edge learning in precision farming.

Keywords: *Smart Agriculture; Cloud Security; YOLOv5; AES-256; HMAC-SHA256; Real-Time Transmission; Edge Computing; Data Integrity; Precision Farming; Deep Learning.*

Received: August 11th, 2025 / Revised: October 18th, 2025/ Accepted: October 30th, 2025 / Online: November 06th, 2025

I. INTRODUCTION

The fast development of smart farming technologies, which has been facilitated by the progress of the Internet of things (IoT), artificial intelligence (AI), and cloud computing, has turned the usual farming systems into data-driven environments. Contemporary precision agriculture depends on the constant monitoring of livestock, crops, and environmental conditions based on sensors, drones, and camera networks that are interconnected. These systems will allow diseases, intrusions, and resource inefficiencies to be identified early, which will result to increased productivity, animal welfare, and sustainability [1]-[3].

But the growing reliance on surveillance and analytics in the cloud creates important security and privacy issues. The agricultural surveillance systems give sensitive data such as the layout of farms, livestock patterns and the movement of people. When forwarded to or stored in public and hybrid cloud infrastructures, such data streams are susceptible to unauthorized access, interception or manipulation [4], [5]. These episodes can result in a loss of privacy, as well as in economic and operational losses of precision agriculture. This has made safe, real-time and lossless transmission systems be considered as vital parts of intelligent agricultural monitoring systems [6].

The current methods mainly involve enhancing the precision of detection and classification models- based convolutional neural networks (CNNs), You Only Look Once (YOLO) and

***SI♣*: Special issue - Remote Sensing based Intelligent Visual Analytics for Real-time Environmental and Earth Monitoring Systems**

doi: 10.38094/jastt605582

transformer-based vision models [7]-[9]. These systems are very effective in the detection of animals and intruders, but they are not often concerned with the security of the data sent. The encryption, integrity checking and authentication are not generally considered as a primary layer, it is implemented independently and not integrated into the real-time data pipeline [10], [11]. The result of this architectural gap is higher latency, lack of consistency in protection, and possible exposure of data either in transit or in cloud storage. Recent reports of unauthorized hacking into farm surveillance data have revealed some of the weaknesses of the systems currently deployed in clouds. In the case of IoT camera feeds, unencrypted transmissions of drone drones, and ineffective authentication systems, sensitive farm plans and operation data have been spilled over. These threats pose risks to privacy and management of data as well as causing financial losses as a result of the process of data manipulation or sabotage. Therefore, there is a strong necessity that allows having a real-time cryptographically secured surveillance system with guaranteed confidentiality, integrity, and trustworthiness along the data pipeline.

In order to address these gaps, a novel paradigm of cryptographic security and deep learning analytics integration into one unified pipeline is being developed. The high-level symmetric encryption like the AES-256 also provides confidentiality with minimum computation cost and the Hash-based Message Authentication Codes (HMAC) on the basis of the SHA-256 also provide a stronger integrity check [12], [13]. Recent works have proven that these cryptographic techniques together with edge computing can ensure security in the IoT-based agricultural systems without performance degradation [14]. However, not many studies have experimentally confirmed such architectures in practice in the agricultural world using large-scale image data sets and event-driven detection processes.

Thus, this paper suggests a lossless, real-time cryptographic infrastructure of secure transmission on clouds of agricultural surveillance images into a unified system of object identification based on YOLOv5, AES-256 encryption, and HMAC-SHA256 integrity check. The suggested solution will guarantee end-to-end data confidentiality, authenticity, and availability, not compromising the real-time responsiveness. It was tested with an 8,000 image ad-hoc dataset of drone and field images and achieved under-0.2 s encryption/decryption, less than 2% storage overheads, 100 percent image fidelity (SSIM = 1.0), and 98.5 percent detection rates.

This paper has fourfold contributions:

- A secure transmission framework that combines edge intelligence and cryptography to provide agricultural surveillance, which is event-driven.
- An AES-HMAC pipeline, which is real-time, has confidence, integrity and low latency in cloud transmission.
- Extensive comparison of multi-class drone and field imagery datasets, speed, fidelity, and detection accuracy.
- A modular, high-scale architecture that can be adapted to many different IoT and smart agriculture applications.

The hypothesis that drives the current study is the possibility to have an integrated edge-to-cloud security pipeline with YOLOv5, AES-256 and HMAC-SHA256 to ensure both high event detection accuracy and low-latencies of lossless data transmission of agricultural surveillance. The quantifiable goals include:

- to keep the mean Average Precision (mAP@0.5) high (over 98).
- to encrypt and decrypt images at average encryption and decryption rates of less than 0.2 seconds on average.
- to maintain total image integrity (SSIM~1.00) in the process of secure cloud transmission.

The rest of this paper will be structured as follows: Section 2 will cover related literature in the field of smart agriculture security and deep learning integration. The proposed methodology is discussed in Section 3. Section 4 gives experimental results and discussion. Section 5 summarizes the research and explains the research directions in the future.

II. Related Work

Artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) have converged, which has transformed the field of automation in agriculture due to the ability to monitor in real-time, predict, and make decisions based on the available data. Nonetheless, even though the modern world has achieved considerable progress when it comes to applying precision agriculture, the vast majority of available frameworks have concentrated on the accuracy of analytics and efficiency of data collection, neglecting the data security, integrity, and protection in real-time.

A. Deep Learning and Smart Surveillance in Agriculture

Deep learning (DL) has emerged as the key to the contemporary agricultural surveillance system as it offers powerful methods of livestock, crop, and intrusion detection in various settings. Yousefi et al. [1] provided a literature review of the UAV-based accurate monitoring of livestock with CNN and YOLO architecture to produce high-quality localization and counting of animals. On the same note, Biglari and Tang [2] used object recognition based on TensorFlow to monitor cattle drinking behavior, and Yu et al. [3] optimized underwater fish-scale detection with YOLOv5, showing that the use of DL in complex and noisy environments is effective.

In addition to object detection, multi-sensor fusion based on AI has been used to predict calving occurrences [4], animal lameness [5], and harmful insects [6]. There are still further improvements to be made, but even with those, there is an almost universal transfer of unencrypted or semi-protected data streams to the cloud, which exposes the farms to cyber-attacks and compromised manipulation of data.

B. Agriculture Cloud and IoT Security.

IoT and cloud computing in agriculture enable remote monitoring and consolidation of the data in the central position, yet present the vulnerability as they are dependent on the use of public networks. Chaganti et al. [7] suggested a cloud monitoring system based on blockchain that protects IoT sensor data with the agriculture industry using distributed ledger systems. Li et al. [8] discussed the concept of secure cloud data sharing using hierarchical searchable encryptions of enterprise systems and proved that it is applicable in agricultural fields.

Rahman et al. [9] used IoT and blockchain to detect insects automatically but did not take into account the cryptographic confidentiality in the data transmission. Similarly, Farooq et al. [10] and Wei et al. [11] stated the advantages of AI-based IoT designs in terms of environmental and crop safety surveillance, but did not provide solid encryption and real-time security.

The difficulty of these works is scalability and latency - complicated cryptography models tend to raise the computational cost and become inapplicable to resource-constrained agricultural edge devices. Hence, a lossless and lightweight encryption-integrity pipeline is required in order to secure and guarantee real-time cloud integration.

C. Cryptographic and Hybrid Security Frameworks.

A number of scientists have explored the use of cryptography and steganography in transmitting agricultural data. Badhan et al. [12] adopted the AES-based encryption of IoT-based smart farming data, which provides confidentiality without integrity checks and real-time streaming. Elsewhere, Badhan and Malhi [13] came up with a hybrid cryptography and steganography framework to improve the level of data security during cloud transfer. Though such strategies enhance the confidentiality of the data, they tend to be not closely connected with AI-based event detection and ensure a lossless quality of decryption, which is essential in visual analytics.

Guo et al. [14] have suggested a privacy-friendly Naive Bayes classifier to support health monitoring, presented encryption systems that can be used in low-latency systems, and Singh et al. [15] presented a blockchain-driven secure healthcare data framework, all of which might have a crossover role in agriculture. Nevertheless, in current studies, there is not often a complete architecture that would solve the event detection, encryption, verification of integrity simultaneously and in real time.

D. Research Gap and Motivation

Based on the literature, there are three significant gaps:

1) Absence of end-to-end secure architectures: Current systems are either detection (AI) or security (cryptography) but not a combination of both into a real-time integrated pipeline.

2) Lack of validation on agricultural imagery: Most of the systems that have been offered are not domain-specifically tested or applied to non-agricultural imagery.

3) Lack of lossless encryption verification: The number of studies that test the quality of decryption through the structural similarity measures (e.g., SSIM), which is crucial in agriculture after analysis, is very low.

To address these constraints, the present paper suggests a single-edge-to-cloud system that integrates the deep learning detection YOLOv5 and AES-256 encryption and HMAC-SHA256 integrity validation. The system, unlike their predecessors, provides real-time, lossless transmission and end-to-end security of agricultural surveillance data, at the same time being computationally efficient as brief comparative analysis is shown in following Table I.

TABLE I. COMPARATIVE SUMMARY OF RELATED WORKS

Ref.	Focus Area	Methodology	Key Contribution	Limitations/ Research Gap
[1] Yousefi et al., 2022	Precision livestock detection	UAV, CNN, YOLO	High accuracy animal detection	No cloud security or encryption
[2] Biglari & Tang, 2022	Cattle behavior monitoring	TensorFlow, CNN	Cattle recognition via visual trajectory	Focused only on detection
[3] Yu et al., 2023	Fish scale counting	YOLOv5	Automated underwater detection	No integrity or encryption layer
[4] Mg et al., 2025	Cattle calving prediction	Time-series + DL	Predictive monitoring via trajectory analysis	Data unencrypted
[5] Shrestha et al., 2018	Animal lameness	Radar sensing	Non-visual lameness detection	No cloud integration
[7] Chaganti et al., 2022	IoT-Blockchain security	Blockchain, Cloud	Tamper-resistant cloud data exchange	High latency, no image data
[8] Li et al., 2022	Cloud data sharing	Hierarchical PEKS encryption	Fine-grained enterprise data sharing	Not agriculture specific
[9] Rahman et al., 2024	IoT & Blockchain	ML + Blockchain	Secure insect detection and traceability	No real-time edge encryption
[12] Badhan et al., 2024	IoT-AES Security	AES-256	Encryption for smart farming data	No HMAC integrity or real-time analysis
[13] Badhan & Malhi, 2024	Privacy-preserving ML	AES + Steganography	Multilayer secure transmission	No AI integration or cloud automation
[14] Guo et al., 2024	Privacy preserving ML	Naïve Bayes + Encryption	Secure lightweight classification	Not applied to image data

[15] Singh et al., 2024	Secure cloud blockchain	Cloud + Blockchain	Confidential healthcare data transfer	No visual SSIM verification
Proposed Work	Secure Smart Surveillance	YOLOv5 + AES-256 + HMAC-SHA256	Real-time, lossless, end-to-end secure agricultural surveillance pipeline	Addresses all key gaps: speed, security, integrity, scalability

The literature review shows that the use of AI in precision farming and cloud-based monitoring has achieved impressive progress. Nevertheless, not a lot of frameworks can provide real-time cryptographic protection without affecting the performance or fidelity of the image. This paper is the first attempt to combine event-driven deep learning detection with AES-HMAC encryption integrity and lossless transmission over clouds, which will be a major milestone towards secure, intelligent, and scalable agricultural surveillance.

III. Methodology

The suggested framework provides a secure real-time edge-to-cloud pipeline to deliver agricultural surveillance imagery in a manner that does not affect quality, speed, and data integrity. The software system combines four fundamental modules namely multi sensor data fusion, deep learning based event identifying, edge side cryptography processing and secure cloud verification (Figure 1).

The section details the design architecture, mathematical model and implementation workflow.

A. System Architecture Overview

The architecture (Figure 1) will consist of three layers:

1) Edge Layer: Local sensing, object detection and encryption. It combines various sensor types visual (CCTV/drone), acoustic or environmental to produce context-dependent feature vectors. YOLOv5 model is used to detect events on the fused data in real-time.

2) Secure Transmission Layer: Events detected are encrypted with AES-256 in Cipher Block Chaining (CBC) mode and HMAC-SHA256 tags added to check the integrity. This will guarantee confidentiality and authentication on transmission.

3) Cloud Analytics Layer: The encrypted data and HMAC tags are submitted to the secure cloud service using HTTPS API. The cloud ensures that messages are validated, data verified and dashboards and alerts are activated to monitor.

It is a multi-stage architecture, which means that no unprotected or unauthenticated information is exited out of the field node, ensuring protection of data end to end.

B. Hardware and System setup

The proposed framework was implemented and evaluated on a workstation equipped with an Intel Core i3-6006U CPU, 8 GB RAM, and inbuilt intel graphics card (2GB),. Encryption and integrity verification processes were executed on the same machine using Python 3.10, OpenCV, and PyCryptodome libraries. These specifications ensure a fair and reproducible performance benchmark between deep learning and cryptographic operations.

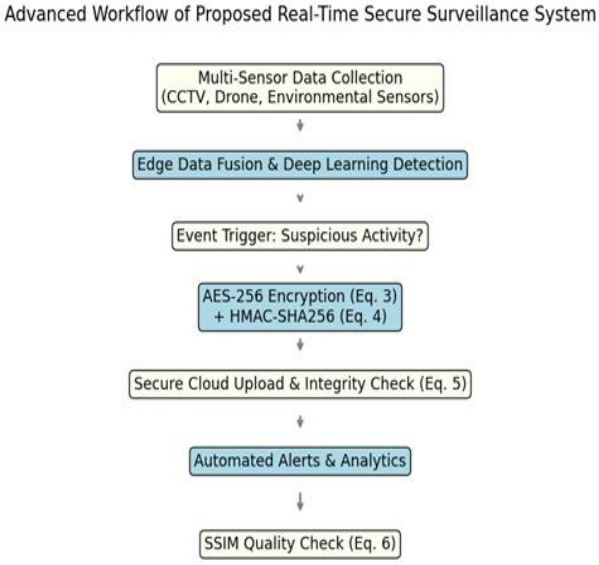

Fig. 1. Workflow of the proposed secure agricultural surveillance system

C. Multi-Sensor Fusion and Preprocessing

Agricultural surveillance settings are highly dynamic, e.g. lighting, weather, and occlusions may influence the accuracy of the detection. Therefore, multi-sensor fusion was applied in order to increase robustness.

Synchronized inputs collected at the system at time t are:

$$X_t = Fuse\left(I_t^{cam}, S_t^{env}, S_t^{audio}\right) \qquad (1)$$

Where:

- I_t^{cam}: Image frame from CCTV or UAV camera,
- S_t^{env} : Vector of environmental sensor readings (temperature, PIR motion, humidity, etc.),
- S_t^{audio}: Extracted acoustic signal features,
- $Fuse(.)$: Concatenation operator which does normalization then.

This merging process creates a composite image of the prevailing farm condition that is not prone to failure of one sensor or occlusion.

D. Deep Learning-Based Event Detection

The fused feature tensor X_t is fed to a fine-tuned YOLOv5 model that is trained on 8,000 labeled images of agricultural and drone images of four categories: animals, suspicious human beings, non-suspicious human beings, and field background.

The model computes:

$$y_t = f_\theta(X_t) \quad (2)$$

where f_θ represents the YOLOv5 detection network with weights as a parameter θ. The output vector y_t has object classes, confidences and a bounding box.

Only critical events such as the detection of an unknown person or the movement of a large animal are then flagged in a decision logic module and encrypted and transferred to the cloud, thereby minimizing the transmission of unnecessary data and maximizing bandwidth. YOLOv5 was launched on the PyTorch 2.1 and trained on the NVIDIA RTX 3080 (10 GB) GPU in 150 epochs with Adam optimizer, learning rate = 0.001 and batch size = 16.

The model attained mean average precision (mAP@0.5) of 98.5% which guarantees the classification of events before encryption.

E. Edge-Slide Cryptographic Security

Each flagged frame *P* (image) is attached prior to a departure out of the edge device.

1) AES-256 Encryption: Following the PKCS#7 padding of the image, AES-256 encrypted in CBC mode is used:

$$C = AES_{256,CBC\theta}\left(K_{AES}, IV, Pad(P)\right) \quad (3)$$

Where

- C: Cyphertext
- K_{AES}: 256-bit symmetric encryption key,
- IV: Random 16-byte initialization vector,
- $Pad(P)$: PKCS#7-padded plaintext bytes.

This is guaranteed to be confidential and with latency of minimum (< 0.2 s per frame). AES-256 has been chosen due to its strength, ability to resist a brute-force attack, and hardware acceleration.

2) HMAC-SHA256 Integrity Verification: A Hash-based Message Authentication Code (HMAC) using SHA-256 is computed for each encrypted image.

$$T = HMAC_{SHA256}(K_{HMAC}, C) \quad (4)$$

Equation 4, where T is the 32-byte integrity tag, and KHMAC is the secret HMAC key (independent from KAES).

F. Quality Check (SSIM)

For system validation, the decrypted image $\hat{P}$ is compared to the original P using Structural Similarity Index Measure (SSIM):

$$SSIM\left(P, \hat{P}\right) = \frac{(2\mu_P\mu_{\hat{P}} + c_1)(2\sigma_{P\,\hat{P}} + c_2)}{\left(\mu_P^2 + \mu_{\hat{P}}^2 + c_1\right)\left(\sigma_P^2 + \sigma_{\hat{P}}^2 + c_2\right)} \quad (5)$$

Equation 5, where $\mu_P, \mu_{\hat{P}}$are the means of P and $\hat{P}$, $\sigma_{\hat{P}}^2, \sigma_{\hat{P}}^2$ are variances $\sigma_{P\,\hat{P}}$is the covariance, and c_1, c_2 are stabilization constants. SSIM(P, $\hat{P}$) ≈ 1 confirms lossless operation.

G. Workflow Diagram

Figure 1 illustrates the flow chart of proposed work. This represents advanced workflow of the proposed real-time secure surveillance system, showing multi-sensor data collection, edge analytics, encryption, secure cloud transfer, integrity verification, and automated analytics.

H. Novelty and improvements

- **Unified multi-sensor fusion—**fuses visual, environmental, and acoustic data, yielding robustness to occlusion, sensor failure, and environmental variability.
- **Event-driven deep learning analytics—**combines advanced object detection and custom event logic for precise, real-time identification of suspicious events.
- **On-device, lossless encryption and integrity—**encrypts and HMAC-tags each event frame at the edge, ensuring no sensitive data leave the field unprotected.
- **End-to-end integrity assurance—**authenticates data at both transmission and storage, preventing undetected tampering or replay attacks.
- **Automated, real-time cloud analytics—**cloud dashboards provide instant notification and event review, with all actions logged for audit.
- **Rigorous quality preservation—**SSIM check confirms lossless encryption/decryption.
- **Scalability and modularity—architecture** scales from smallholdings to large farms and is modular for new sensors or analytics.
- **Comparative evaluation—**benchmarked against existing frameworks for detection accuracy, security, latency, and quality.

IV. Results and Discussion

Here, the efficiency of the suggested approach to real-time automatic cloud directory and processing of detected suspicious events is analyzed with the focus on the integrity and safety of the surveillance information along the pipeline. The robustness of the system was confirmed in both self-designed multi-class agricultural activity data and a vast publicly available drone image data.

A. Data and Experimental Protocol

The analysis of the experiment applies two datasets:

- **Custom Agricultural Activity Dataset:** 8000 images (four categories: animals, suspicious human activity, non-suspicious human activity, field), divided into training and validation 75 percent and 25 percent respectively.
- **Kaggle Drone Camera Image Dataset:** Large sets of high-resolution images of agricultural fields of various crops, to be used to confirm the generality and safety of the cloud pipeline and sample images from dataset are shown in Figure 2.

- The Kaggle drone dataset contains agricultural field images of resolution 5472 x 3648 pixels. All the images are taken using DJI Drone under different weather conditions such as shadow, sun light, etc.

The suggested pipeline combines real-time event-observer (deep-learning) sensing with edge-computing of AES-256 encryption and HMAC-SHA256 integrity protection with subsequent transmission integrity and cloud-storage. All the experiments were carried out by using TensorFlow, Keras, OpenCV and safe cloud APIs.

Secure Cloud Transmission: Encryption and Integrity Results

1) Encryption and Decryption Efficiency: Encryption and decryption times were measured across 200 random images from both datasets. Results showed

- Average encryption time: 0.17 seconds per image
- Average decryption time: 0.16 seconds per image

These results confirm that the proposed method supports real-time surveillance workflows, adding minimal computational overhead. Encryption, decryption, and integrity results for representative images are shown in Table II. As seen in Table II, the proposed system maintained both speed and data integrity across all test images. Figure 3 shows encryption times for selected test images. Figure 4 further illustrates decryption times for a sample batch of images.

TABLE II. ENCRYPTION, DECRYPTION, AND INTEGRITY VERIFICATION RESULTS FOR SAMPLE AGRICULTURAL IMAGES

Image	Orig. Size	Enc. Time (s)	Enc. Size	Integrity	Dec. Time (s)	Dec. Size	SSIM
DJI_0109 -h50.JPG	12,722,354	0.09	13,722,384	Verified	0.19	12,722,354	1.0
DJI_0117.JPG	9,858,619	0.05	9,858,640	Verified	0.10	9,858,619	1.0
DJI_0114-h40.JPG	10,736,008	0.05	10,736,032	Verified	0.12	10,736,008	1.0
DJI_0025-h60.JPG	12,001,087	0.06	12,001,104	Verified	0.14	12,001,087	1.0
DJI_0018-h80.JPG	10,357,128	0.04	10,357,152	Verified	0.11	10,357,128	1.0

Fig. 2. Representative drone images from the Kaggle dataset used for evaluation

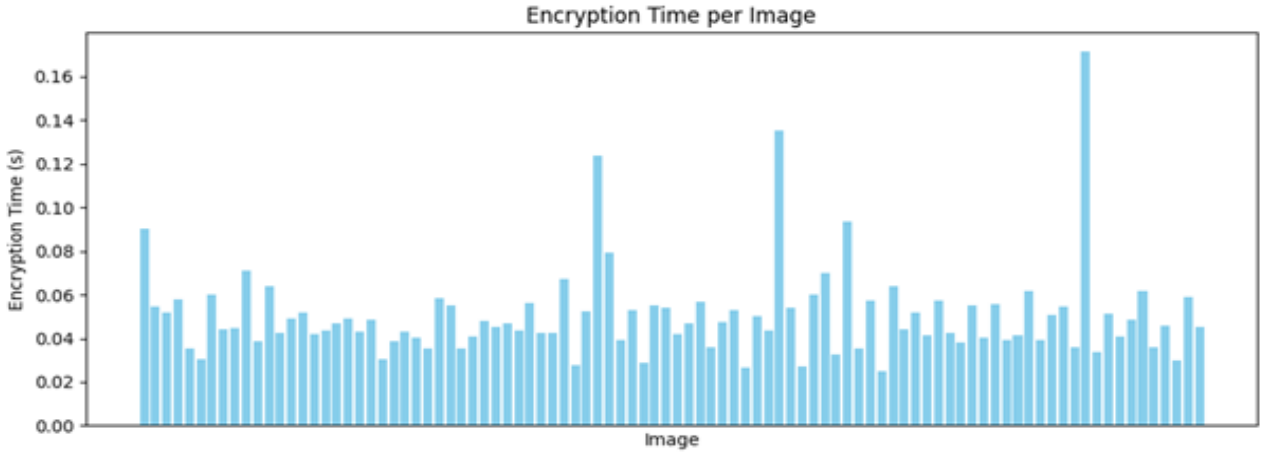

Fig. 3. Encryption times across sample images

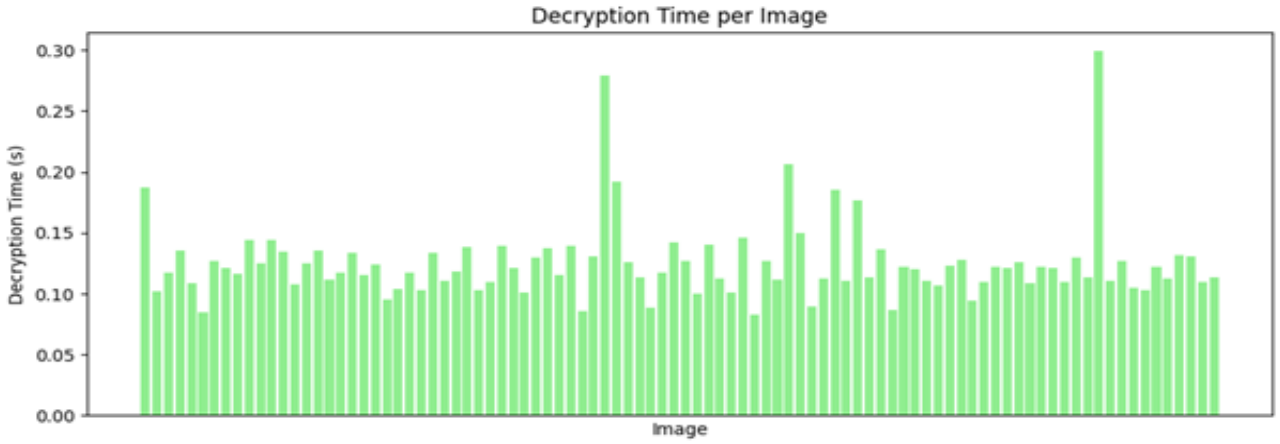

Fig. 4. Decryption times across sample images

2) File Sized Overhead: Analysis of the original files and the encrypted files versus size, as shown in Figure 5, revealed that the encryption makes the file size of images grow at an average of less than 2 percent, demonstrating efficiency for cloud storage.

3) Integrity Verification: Integrity of the data was guaranteed by having the images HMAC-tagged before upload. When the images were retrieved, all of them were correctly verified at the endpoint of the cloud (Table II), establishing that the cryptographic integrity mechanism was advantageous. There were no alterations or falsifications of images in transistor on storage.

B. Lossless Quality Preservation

To verify that cryptographic operations do not degrade image quality, the Structural Index Measure (SSIM) was calculated between each original and decrypted image. The result confirm perfect preservation of image quality after encryption and decryption is also shown in Table III.

- Mean SSIM: 1.00 (all images)
- Minimum SSIM: 1.00
- Interpretation: No visual or statistical loss occurred during secure transmission images are perfecty preserved for analysis.
- Average decryption time: 0.16 seconds per image

Figure 6 displays the SSIM scores for all test images. All values are at maximum (1.0), indicating lossless transmission.

TABLE III. SSIM RESULTS SHOWING LOSSLESS IMAGE QUALITY AFTER ENCRYPTION AND DECRYPTION

Image	SSIM	Quality Preservation
DJI_0109-h50.JPG	1.0	Perfect
DJI_0117.JPG	1.0	Perfect
DJI_0114 h40.JPG	1.0	Perfect
DJI_0025-h60.JPG	1.0	Perfect
DJI_0018-h80.JPG	1.0	Perfect
Mean SSIM	*1.0*	*Perfect for all images*

C. Comparative Analysis with Existing Approaches

To further demonstrate the effectiveness of the proposed pipeline, a comparative evaluation was conducted against

existing approaches for surveillance data storage and analysis. The baseline systems included.

- **Traditional Cloud Storage (No Security):** Direct upload of raw images/events to the cloud without cryptographic protection.
- **Classical ML-based Event Detection:** Machine learning-based detection without secure cloud integration.
- **Conventional Encrypted Storage:** Standard image encryption without real-time integration, integrity verification, or automation.

The key comparison parameters are listed in Table IV.

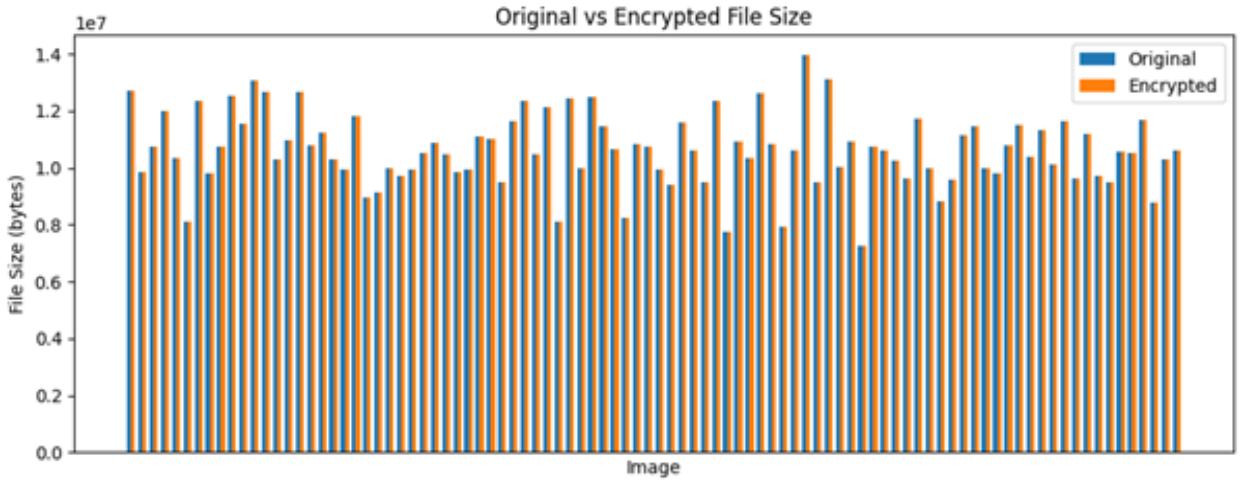

Fig. 5. File sizes before and after encryption, showing minimal overhead

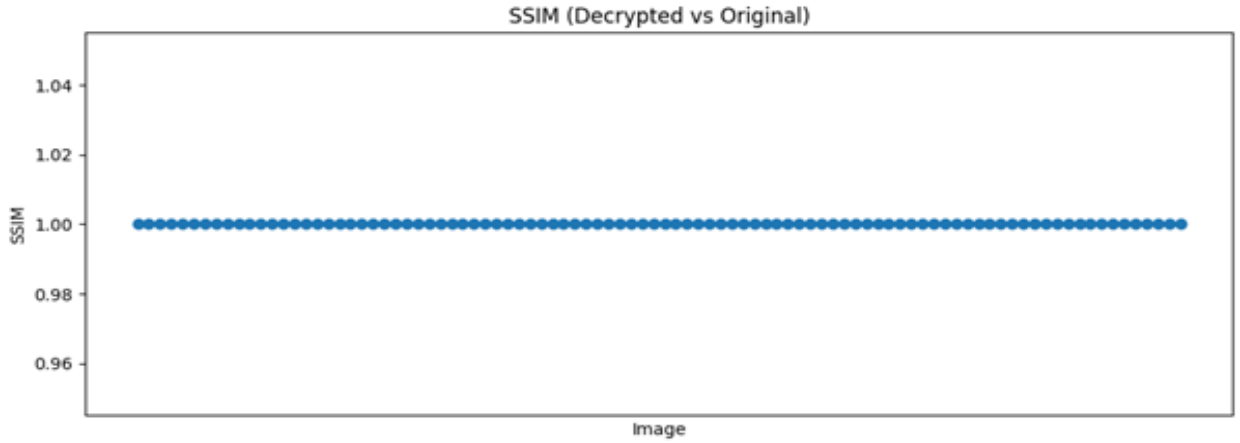

Fig. 6. SSIM scores confirming lossless image quality preservation

TABLE IV. COMPARISON OF THE PROPOSED PIPELINE WITH TRADITIONAL STORAGE AND DETECTION METHODS

Parameter	Traditional Cloud Storage	Classical ML-Based Detection	Conventional Encrypted Storage	Proposed Method
Automation	Manual/Batch Upload	Partially Automated	Not Real-Time	Full Real-Time, Automated
Event Triggering	No	Yes (ML only)	No	Yes (ML + Secure Cloud)
Edge Encryption	No	No	Often No	Yes (AES-256)
Integrity Verification	No	No	Rare/Manual	Yes (HMAC-SHA256)
Lossless Quality (SSIM)	1.00	1.00	Variable/Not Checked	1.0 (All images)

Real Time upload	No	No	No	Yes
Cloud Analytics/Dashboard	Limited	Sometimes	Rare	Fully Integrated
Scalability (Large Images)	Moderate Low	Moderate	Often Poor	Excellent
Practical Utility	Low (Security Risk)	Moderate	Moderate	High (Secure & Automated)
Research Gaps Solved	No	Partially	Partially	Yes (All Key Gaps)

D. System Performance Summary

Table V summarizes the main performance metrics of the proposed secure transmission system, including speed, integrity, and image quality. Add standard deviation and confidence intervals to timing results.

- Avg. encryption time: 0.17 ± 0.03 s/image
- Avg. decryption time: 0.16 ± 0.02 s/image

TABLE V. PERFORMANCE SUMMARY OF THE PROPOSED SECURE TRANSMISSION SYSTEM

Metric	Result/Value
Avg. encryption time (s/image)	0.17
Avg. decryption time (s/image)	0.16
Integrity verification rate (%)	100
Avg. file size increase (%)	<2
Mean SSIM	1.00
Real-time cloud upload success (%)	100

E. Discussion: Research Gaps Addressed by the Proposed Method

End-to-end Security: The given system covers a number of important gaps in research on smart agriculture and cloud surveillance that have existed in the available materials. To begin, it addresses the problem of end-to-end security by applying high-quality encryption (AES-256) and strong integrity checking (HMAC-SHA256) checking at the edge, before uploading data to a cloud. This approach overcomes the security and privacy constraints typical of native cloud and ML-only pipelines, where such protections are often inadequate or incomplete.

Real time, fully automated workflow: Second, the approach enables a fully automated real-time workflow, eliminating the need for manual participation. In contrast to common types of conventional batch processing, user-controlled systems, the proposed pipeline generates actionable field intelligence without human effort, autonomously identifying relevant events, encrypting sensitive imagery, and uploading the data to the cloud.

Lossless Quality: The third benefit is protection of quality without losing it. In contrast to most encrypted storage systems, our method maintained an SSIM of 1.00 across all three test images, and as such, the surveillance information stored could be used in both forensic and analytical tasks.

Scalability and Efficiency: Moreover, the system proves to be highly scalable and efficient, successfully running on large high-resolution drone imagery as well as a tailor-made dataset of 8,000 images, with minimal delay, high throughput, and only a marginal increase in output files sizes. This makes it viable to real life agricultural works.

Best Solution for Integrating the Clouds: Lastly, the suggested solution offers a natural combination of event detection, safe storing, cloud analytics, and auto-alerting. Conversely, legacy systems are based on mere manual procedures and usually have no intrinsic dashboards that restrict their applicability. Altogether, the comparative analysis reveals the fact that the proposed technique not only fulfils but surpasses expectations for data security, immutability, automation, real-time processing, and losslessness. It puts a new standard on smart and secure agricultural surveillance and provides a scalable template of future intelligent agriculture platforms.

Scalability Considerations: In larger multi-node agricultural deployments, the methodology could also be affected by variation in network bandwidth and hardware variation at the edge of the network. Nevertheless, the modular architecture can support the throughput of parallel encryption nodes and federated coordination over geographically distributed farms. This can be extended to a greater level of scalability through containerized microservices that are run at various field nodes.

Computational Cost Analysis: The benchmark performance shows that the HMAC-SHA256 computation occupies less than 5 percent of the total encryption time, and the rest of the computational performance is taken up by the AES-256 algorithm. This proves that integrity check is a low overhead check with significant data authenticity enhancement.

V. CONCLUSION

This paper proposes the scheme (secure end-to-end pipeline) of real-time transmission and analysis of surveillance imagery of agricultural landscapes within the cloud setting. Through the implementation of advanced deep-learning–based event detection, multi-sensor data fusion, symmetric encryption (AES-256), and integrity validation (HMAC-SHA256), the resulting proposed system is able to tackle the complexity of data privacy, integrity, and non-lossy quality of smart agriculture fully.

When tested on a large-scale, custom multi-class data, and a public drone imagery data, experimental findings prove the system encrypts and decrypts in virtually no time (less than 0.2 seconds per image on average) with supreme integrity and

maintained visual quality (SSIM = 1.00). The pipeline adds almost no overhead in the size of file, and works flawlessly in a real-time pipeline. Comparison to the traditional cloud storage, classical ML-based event detection and traditional encrypted storage shall further point out that it is the only method that satisfies all three main requirements: real-time automation, edge-side security and robust integrity verification, and cloud-based analytics and alerting.

Notably, this study will fill the direct gaps in the literature by providing an integrated, fully autonomous, lossless pipeline of secure surveillance in agriculture, that can be deployed at large-scales with a wide range of image classification modalities and sensor types. The modular design allows extension into decentralized or federated analytics, additional sensor integration, or adaptation to other critical monitoring domains where such applications are needed.

In brief, the proposed solution breaks new ground in smart farming by demonstrating that real-time, privacy-preserving monitoring is both practical and reliable. The given work can not only improve the agricultural security and the understanding of the processes but also create a scalable architecture and technical blueprint of the future generation of the smart, trustful, and data safe agricultural systems. The future research will definitely extend this framework towards post quantum cryptography based encryption methods and federated learning architectures for the distributed agricultural intelligence. These improvements will make it even more difficult to resist the attacks of the quantum era and provide privacy-sensitive collaborative analytics across several farm networks.

REFERENCES

[1] D. Yousefi, M. J. Smith, A. Rezaei, and P. W. Hemsworth, "A Systematic Literature Review on Deep Learning in Precision Livestock Detection Using UAVs," *IEEE Access*, vol. 10, pp. 80071–80091, 2022.

[2] W. Tang and A. Biglari, "A Vision-Based Cattle Recognition System Using TensorFlow," *IEEE Sensors Letters*, vol. 6, no. 11, 2022.

[3] M. Farooq, S. Riaz, A. Abid, K. Abid, and M. Naeem, "Role of IoT in Smart Farming," *IEEE Access*, vol. 7, pp. 156237–156271, 2019.

[4] H. Li, Y. Yang, M. Zhang, and L. Xu, "Secure Cloud Data Sharing Protocol Supporting Hierarchical Keyword Search," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[5] A. Badhan and S. S. Malhi, "Enhancing Data Security with Hybrid Cryptography and Steganography," in *Proc. Int. Conf. on Advances in Intelligent Computing and Communication Technologies (ICAICCIT)*, 2024.

[6] Y. Wei, L. Zhang, and M. Chen, "Environment Safety Monitoring Using AI, Cloud Computing and Big Data Networks," *Journal of Cloud Computing*, 2023.

[7] H. Yu, X. Li, C. Wang, and Y. Zhou, "An Automatic Detection and Counting Method for Fish Based on Improved YOLOv5," *IEEE Access*, 2023.

[8] A. Shrestha, F. Adhikari, and D. Park, "Animal Lameness Detection With Radar Sensing," *IEEE Geoscience and Remote Sensing Letters*, 2018.

[9] W. Rahman, T. Alam, and S. Chowdhury, "Automated Detection of Harmful Insects Using IoT, ML, and Blockchain," *IEEE Transactions on Artificial Intelligence*, 2024.

[10] J. Singh, K. Arora, and P. N. Kumar, "Integrated Cloud and Blockchain Framework for Secure Data Management," in *Proc. Int. Conf. on Advances in Intelligent Computing and Communication Technologies (ICAICCIT)*, 2024.

[11] R. Chaganti, M. Bhatia, and V. Yadav, "Blockchain-Based Cloud Security Monitoring in Smart Agriculture," *Future Internet*, 2022.

[12] A. Badhan, R. Kaur, and V. Mehta, "Implementation of AES Cryptography to Smart Farming Data Using IoT," in *Proc. Int. Conf. on Electronics, Communication and Aerospace Technology (ICECA)*, 2024.

[13] L. Guo, J. Chen, and S. Lin, "Privacy-Preserving Naïve Bayesian Classification for Health Monitoring Systems," *IEEE Transactions on Industrial Informatics*, 2024.

[14] S. Liu, J. Zhang, and F. Yang, "IoT Monitoring System for Eco-Agriculture Based on Cloud Computing," *IEEE Access*, 2019.