



AI-Enabled IoT Security Architecture For Real-Time Intrusion Detection in Maize Farms using Custom You Only Look Once (Yolo) Models and GSM Alert Systems

Excellence Favor¹, Omia Moses¹, Abubakar Abdulkarim^{1,2*}, Yinusa Ademola Adediran³

¹Department of Electronics and Computer Engineering, Soroti University, Uganda.

²Department of Electrical, Telecommunication and Computer Engineering, Kampala International University, Uganda

³Department of Electrical and Electronics Engineering, University of Ilorin, Nigeria.

***Corresponding author:** abiczarewa@gmail.com; +256771050135; ORCID: 0000-0003-0303-6327

DOI: <https://doi.org/10.xxxx/xxxx>

Keywords:

*Deep Learning-Based Detection;
Edge Computing;
Intelligent Surveillance Systems;
Smart Agriculture;
Wireless Sensor Networks;
YOLOv8*

Article History:

Received: 5 September 2026

Revised: 10 October 2026

Accepted: 12 October 2026

Published: 15 October 2026

Article Info:

Homepage: <https://zjeet.com.ng>

Volume: 15, No. 1, 2026

Pages: 82-101

ABSTRACT

Maize production in resource-constrained agricultural environments is increasingly threatened by human intrusion, livestock encroachment, bird infestation, and tampering with field-deployed monitoring infrastructure, resulting in crop losses, reduced productivity, and operational inefficiencies. Conventional security approaches, including manual guarding, perimeter fencing, and motion-triggered alarm systems, lack contextual intelligence, suffer from high false-alarm rates, and provide limited real-time responsiveness. This study presents an AI-enabled Internet of Things (IoT) security architecture for real-time intrusion detection in maize farms, integrating a custom-trained You Only Look Once version 8 (YOLOv8) object detection model, lightweight face-recognition algorithms, GSM-based communication, and edge computing implemented on a Raspberry Pi 5 platform. The system autonomously performs motion sensing, image acquisition, object classification, identity verification, alert generation, and dashboard-based event monitoring without cloud dependency. Experimental evaluation through laboratory validation and controlled field simulations demonstrated strong detection capability and operational robustness. The model achieved an overall detection accuracy of 84%, human detection precision of 0.856, recall of 1.000, and a mean Average Precision (mAP@50) of 0.848, confirming reliable multi-class detection performance. F1-scores of 0.741 and 0.801 for animal and bird classes, respectively, further indicate robust generalization under dynamic agricultural conditions. The system maintained an average end-to-end response latency of approximately 2 s, satisfying real-time operational requirements. To formalize integrated system effectiveness, performance is analytically modelled as a function of detection confidence, model generalization, communication reliability, environmental robustness, intrusion risk, and cumulative latency. Designed for low-connectivity rural environments, the architecture offers a scalable, low-cost, and context-aware solution for intelligent agricultural security in developing regions.

1. INTRODUCTION

Maize production in rural and resource-constrained regions remains a critical pillar of food security,

household income, and national agricultural economies. However, its sustainability is increasingly threatened by persistent and multifaceted security challenges, including human intrusion, livestock

encroachment, and deliberate interference with field-deployed equipment. These threats contribute to substantial yield losses, increased operational costs, and heightened vulnerability among smallholder and medium-scale farmers, who often lack access to structured surveillance infrastructure and intelligent farm protection systems [1]. Empirical observations conducted during preliminary field assessments confirmed recurrent intrusion events involving unauthorized individuals, as well as animals such as cattle, goats, pigs, monkeys, and grain-feeding birds, each contributing to measurable crop destruction and post-harvest losses [2].

Conventional deterrent mechanisms, including scarecrows, manual guarding, and basic perimeter fencing, remain largely inadequate in addressing the dynamic and evolving nature of these threats. These approaches are inherently limited by their inability to provide continuous monitoring, contextual awareness, and timely response capabilities. Furthermore, they lack adaptive intelligence, resulting in inefficiencies, delayed interventions, and increased labor dependency. As a result, there is a compelling need for intelligent, automated, and resilient surveillance systems capable of delivering real-time situational awareness and decision support in agricultural environments [3], [4].

Recent advances in Internet of Things (IoT) technologies, edge-based artificial intelligence, and low-power communication systems have created new opportunities for transforming agricultural monitoring and security. Embedded computing platforms, such as the Raspberry Pi 5, now provide sufficient computational capacity to support real-time machine learning inference directly at the edge, thereby eliminating reliance on cloud-based processing and reducing latency [5]. In parallel, deep learning frameworks, particularly the You Only Look Once (YOLO) family of object detection models, have demonstrated high accuracy and efficiency in real-time visual recognition tasks, making them well suited for deployment in dynamic and resource-constrained field environments [6], [7].

Despite these technological advancements, existing smart agriculture systems have predominantly focused on productivity optimization domains such as irrigation management, pest detection, and yield prediction, with limited emphasis on comprehensive farm security. This gap is especially pronounced in the Uganda, where unreliable internet connectivity, harsh environmental conditions, and limited infrastructure impose additional constraints on technology adoption. Consequently, there remains a critical need for integrated, context-aware architectures that combine IoT sensing, edge intelligence, and resilient communication mechanisms to provide reliable, real-time intrusion detection and response.

In response to these challenges, this study proposes an AI-enabled IoT security architecture for real-time intrusion detection in maize farms. The system integrates multi-sensor inputs, a custom-trained YOLOv8 object detection model, lightweight face-recognition algorithms, and GSM-based communication deployed on a Raspberry Pi 5 edge platform. This architecture enables autonomous detection, classification, and notification of intrusion events, thereby enhancing farm security, reducing losses, and supporting timely farmer intervention. The proposed approach emphasizes offline capability, low-cost deployment, and adaptability to rural environments, making it particularly suitable for developing-country contexts.

This work aligns with global and regional development priorities, contributing to the achievement of the Sustainable Development Goals (SDGs), Uganda's National Development Plan IV (NDP IV), Africa Agenda 2063, and Vision 2040 by strengthening agricultural resilience, food security, and technological innovation. Furthermore, it supports regional frameworks under the East African Community that promote agricultural modernization and innovation, while advancing Soroti University's strategic vision of leveraging engineering solutions for community transformation and sustainable rural development.

1.1 Motivation and problem

A critical evaluation of existing field practices reveals several persistent challenges that undermine both crop protection and the integrity of farm-installed systems. These include frequent unauthorized entry by individuals seeking to harvest or steal maize, as well as recurrent livestock and wildlife intrusion leading to extensive crop damage. In addition, deployed hardware components; including cameras, sensors, and embedded processing units are highly susceptible to tampering, displacement, or theft, thereby compromising system reliability and continuity of operation.

Traditional monitoring systems, particularly those based solely on passive infrared (PIR) sensing, suffer from high false-alarm rates due to their inability to distinguish between relevant and irrelevant motion events. This lack of classification intelligence reduces system credibility and leads to inefficient or delayed responses. Moreover, the widespread absence of stable internet connectivity in rural farming regions limits the effectiveness of cloud-dependent surveillance solutions, necessitating the development of autonomous, edge-based systems capable of operating independently of broadband infrastructure.

These limitations highlight the need for a context-aware, classification-driven security framework that can deliver accurate, real-time intrusion detection while ensuring reliable communication under constrained conditions. The system proposed in this study addresses these challenges through the integration of a custom YOLOv8 object detection model, lightweight face-recognition algorithms for identity verification, GSM-based SMS alerting for dependable communication, and a web-based interface for monitoring and data management. The operational workflow of the system—including motion detection, image acquisition, object classification, identity verification, alert generation, and data logging is illustrated in Figures 3 and 4, demonstrating a unified and intelligent security pipeline for maize farm environments.

1.2 Overview of system architecture

The proposed system adopts a structured, multi-layer architecture designed to ensure robustness, scalability, and real-time performance in resource-constrained agricultural environments. The architecture is organized into four tightly integrated layers, each responsible for a critical stage in the intrusion detection and response pipeline.

The Sensing Layer forms the foundational interface between the physical environment and the digital system. It comprises a Passive Infrared (PIR) motion sensor, a Light Dependent Resistor (LDR), and a USB camera interfaced with a Raspberry Pi 5. This layer enables continuous environmental monitoring, motion-triggered image acquisition, and adaptive sensing under varying lighting conditions, thereby ensuring reliable data capture in dynamic farm environments Figure 3.

The Perception Layer constitutes the intelligence core of the system. It integrates a custom-trained YOLOv8 object detection model, fine-tuned using localized maize farm datasets, alongside an optimized face-recognition module for identity verification. This combination enables accurate classification of detected entities into meaningful categories, including authorized personnel, intruders, livestock, and birds. By incorporating both object detection and identity recognition, the system significantly reduces false alarms and enhances contextual awareness.

The Communication Layer ensures reliable and timely dissemination of intrusion alerts. A SIM900 GSM module is employed to transmit real-time Short Message Service (SMS) notifications to the farmer, enabling immediate response even in regions with limited or no internet connectivity. This design choice is particularly critical for rural deployments, where dependence on broadband infrastructure is often impractical.

The Application Layer provides an interactive web-based interface for real-time monitoring, visualization of detection events, and storage of historical intrusion logs. This layer enhances usability by enabling farmers

to remotely access system outputs, review past events, and make informed decisions regarding farm security.

System coordination across these layers is achieved through an integrated processing pipeline. Motion detection triggers image capture, which is subsequently processed by the machine learning models for classification and identity verification. Based on the classification outcome, the system executes decision logic to trigger alerts, activate deterrent mechanisms where applicable, and log the event in the database. The overall system architecture and data flow are illustrated in Figures 1 and 3, while the operational workflow is presented in Figure 4.

Supporting evaluation artefacts including precision–recall curves, F1-score analysis, confusion matrix, and representative detection outputs (Figures 5–17) are incorporated in subsequent sections to rigorously validate system performance. Collectively, these components establish a unified, intelligent security pipeline capable of real-time detection, classification, notification, and user interaction in maize farm environments.

2. RELATED WORKS

2.1 Security systems in agriculture

IoT-based agricultural monitoring systems have traditionally relied on motion sensing technologies combined with basic alert mechanisms such as GSM notifications [11], [12]. While these systems provide foundational monitoring capabilities, their lack of classification intelligence results in high false-alarm rates, often triggered by non-threatening environmental movements such as wind or small animals. This leads to excessive, non-actionable alerts, ultimately reducing user trust and system effectiveness.

Furthermore, existing agricultural security solutions largely overlook the protection of deployed equipment, including sensors, cameras, and embedded controllers. As observed in field-based studies, equipment tampering and theft represent a significant yet underexplored vulnerability in smart farming systems. This gap highlights the need for

comprehensive security frameworks that address both crop protection and infrastructure integrity.

2.2 Deep learning for object recognition in agriculture

Deep learning techniques, particularly those based on convolutional neural networks, have significantly advanced object detection capabilities in agricultural applications. Among these, the YOLO (You Only Look Once) family of models is widely recognized for its ability to achieve high detection accuracy with low inference latency, making it suitable for real-time deployments [7].

When trained using localized datasets that reflect the specific environmental and operational conditions of maize farms, YOLO-based models demonstrate superior performance compared to conventional machine vision approaches. In this study, the use of a custom-trained YOLOv8 model enables robust detection of multiple classes, including humans, livestock, and birds.

Performance evaluation artefacts including precision–recall curves (Figure 16), F1-score trends (Figure 17), and confusion matrix analysis (Figure 18)—provide detailed insights into model behaviour. These results reveal strong detection performance for human classes, while comparatively lower recall for animal classes reflects dataset imbalance and environmental variability an observation consistent with real-world deployment conditions.

2.3 IoT–GSM systems for rural monitoring

In rural and resource-constrained environments, GSM-based communication remains a reliable and widely adopted solution for remote monitoring systems [13], [14]. The integration of SIM900 GSM modules enables the transmission of SMS alerts without reliance on internet connectivity, thereby ensuring consistent system operation in areas with limited network infrastructure.

Although prior studies have explored the use of IoT and GSM technologies for agricultural monitoring, these implementations typically lack integration with advanced machine learning models. As a result, they

provide limited intelligence and are unable to distinguish between different types of intrusion events. The architecture proposed in this study addresses this limitation by combining IoT sensing, edge-based AI, and GSM communication into a unified and context-aware system.

2.4 Research gaps

A critical analysis of existing literature reveals several key limitations:

The absence of fully integrated agricultural security architectures that combine sensing, intelligence, communication, and user interaction within a unified framework.

Limited incorporation of real-time intruder classification, resulting in high false-alarm rates and reduced system reliability.

Insufficient empirical validation of systems deployed in developing-country contexts, particularly under real environmental conditions.

Minimal consideration of equipment security and system tampering, despite its practical significance in field deployments.

The system proposed in this study directly addresses these gaps through its multi-layer architecture, real-time AI-driven classification, GSM-based communication, and comprehensive performance validation. The integration of these components, as illustrated in Figures 1–4 and validated through experimental results, represents a significant advancement toward intelligent and resilient agricultural security systems.

3. METHODOLOGY

The methodological framework adopted in this study is grounded in a Design Science Research (DSR) paradigm, integrating system design, machine learning model development, iterative prototyping, and empirical validation. This approach ensures that the proposed AI-enabled IoT security architecture is both scientifically rigorous and practically deployable within real-world maize farm environments.

The methodology is structured into five interrelated phases: (i) requirements analysis, (ii) system modelling, (iii) component selection and integration, (iv) prototyping and testing, and (v) field simulation and validation.

3.1 Requirements analysis

The initial phase involved comprehensive problem identification through field observations and stakeholder engagement, including interviews with local farmers and agricultural practitioners. As observed in real maize farming environments in Soroti, the system must address recurrent and context-specific threats such as:

- a. Nighttime human intrusion for crop theft
- b. Livestock incursions (cattle, goats, pigs)
- c. Bird attacks during grain maturation
- d. Tampering or theft of deployed sensing and computing equipment

Based on these observations, the following system requirements were established:

- i. Autonomous, real-time detection of multiple intrusion categories
- ii. Accurate classification under dynamic environmental conditions
- iii. Independence from broadband infrastructure through GSM-based communication
- iv. Low-cost, energy-efficient hardware suitable for rural deployment
- v. Edge computing capability for local processing of image streams
- vi. Integrated architecture linking sensing, inference, communication, and monitoring

3.2 System design modelling

The system was modelled using structured design methodologies to ensure coherence across functional, logical, and physical layers. The architectural representation is illustrated in Figure 1, which presents a four-layer AI-enabled IoT system integrating sensing, perception, communication, and application modules.

Supporting modelling artefacts include:

Fig. 1: System Block Diagram (Section 3.2) – overall architecture

Fig. 2: Prototype Setup (Section 3.4) – physical implementation layout

Fig. 3: Data Flow Diagram (Section 4.2) – operational logic pipeline

Fig. 14: System Flowchart (Section 4.5) – decision-making sequence

These artefacts collectively define the system workflow:

PIR Trigger → Image Capture → YOLO Inference → Classification → GSM Alert → Dashboard Logging
This modelling process ensured design consistency prior to hardware realization.

Figure 1 illustrates a four-layer AI-enabled IoT security architecture in which sensors capture field inputs, a Raspberry Pi 5 executes YOLOv8 detection and face recognition, GSM communication transmits alerts, and a web dashboard provides real-time monitoring, enabling autonomous, reliable maize-farm intrusion detection.

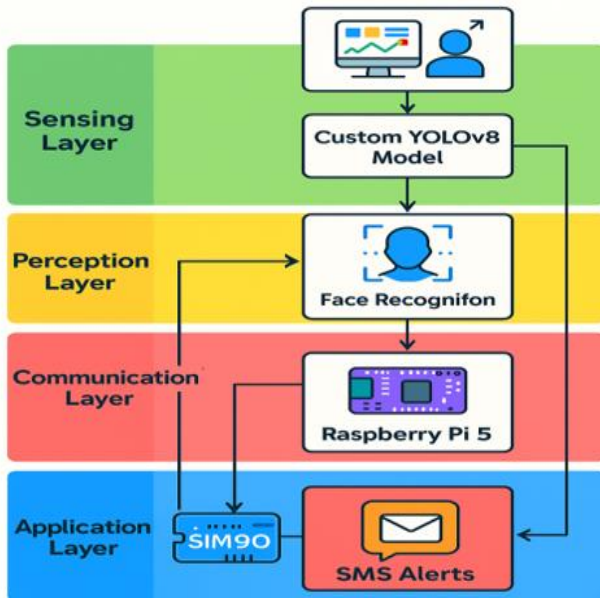


Fig. 1: AI enabled IoT Farm security system Architecture

3.3 Hardware and software component selection

A rigorous selection process was undertaken to ensure optimal performance under rural deployment constraints, considering cost, availability, energy efficiency, and environmental robustness.

Hardware components (Table 1) include:

1. Raspberry Pi 5 (edge processing unit)
2. PIR motion sensor (trigger mechanism)
3. LDR sensor (lighting adaptation)
4. USB camera (image acquisition)
5. SIM900 GSM module (communication)
6. Relay and buzzer modules (actuation and alerting)

Table 1 presents the hardware architecture underpinning the proposed AI-enabled IoT security system, detailing component specifications, functional roles, interfacing, power requirements, and deployment relevance. It highlights the system's cost-effectiveness, modular integration, and suitability for real-time operation in resource-constrained agricultural environments.

Software components (Table 2) include:

1. Python 3.11 (core processing environment)
2. YOLOv8 framework (object detection)
3. ONNX-optimized face recognition module
4. Flask web server (backend)
5. PHP/JavaScript dashboard (frontend interface)
6. Roboflow (dataset annotation and augmentation)

Each component was evaluated for performance efficiency, latency, reliability, and compatibility with edge deployment constraints.

Table 1: Hardware Architecture, Functional Roles, and Deployment Characteristics of the Proposed AI-IoT Farm Security System

S/N	Component	Specification	Functional Role	Interface / GPIO Mapping	Power Requirement	Operational Contribution	Estimated Cost (UGX)	Deployment Significance
1	Raspberry Pi 5	Model B, 8GB RAM, Quad-core CPU	Central processing and edge AI computation	USB, GPIO, UART	5V / ~5–7W	Executes YOLOv8 inference, controls system logic	350,000	Enables real-time edge intelligence without cloud dependency
2	USB Camera	8MP, 1080p resolution	Image/video acquisition	USB Interface	5V / ~2W	Provides visual data for object detection	120,000	Critical for accurate detection and classification
3	PIR Motion Sensor	HC-SR501	Motion detection trigger	GPIO 17	5V / <1W	Activates system upon motion detection	15,000	Reduces unnecessary processing and energy consumption
4	LDR Sensor	Photoresistor	Ambient light sensing	GPIO 23	5V/negligible	Controls lighting conditions dynamically	5,000	Enhances night-time detection reliability
5	Relay Module	5V Relay	Actuation of external devices (e.g., bulb)	GPIO 24	5V / ~1W	Enables automated lighting control	10,000	Supports adaptive environmental response
6	GSM Module	SIM900 (/dev/ttyAMA0)	SMS communication	UART (TX/RX)	5V / ~2W	Sends real-time alerts to farmer	80,000	Ensures operation in low/no internet environments
7	Buzzer	Active buzzer	Audible alert mechanism	GPIO 25	5V / <1W	Provides immediate local alert	5,000	Enhances deterrence and real-time awareness
8	Illumination Bulb	12W AC	Night illumination	Relay-controlled	220V AC	Improves visibility during night detection	12,500	Ensures system robustness in low-light conditions

Table 2 outlines the integrated software stack supporting the system, specifying tools, frameworks, functional roles, and system-layer interactions. It demonstrates how artificial intelligence, embedded processing, and web technologies collectively enable real-time detection, communication, and user interaction within the proposed agricultural security architecture.

3.4 Prototyping and Laboratory Testing

A functional prototype was developed in accordance with the architecture illustrated in Figure 2 and subjected to comprehensive laboratory testing to

validate system performance and reliability. The evaluation focused on critical operational aspects, including GPIO interfacing and signal integrity, camera streaming stability, PIR sensor sensitivity calibration, GSM communication reliability, and web server responsiveness under varying loads. These controlled tests facilitated systematic optimization of key system parameters, such as detection thresholds, sampling intervals, and computational load distribution on the Raspberry Pi platform. Collectively, the results ensured stable operation, efficient resource utilization, and readiness for subsequent field deployment under real-world agricultural conditions.

Table 2: Software Stack, Functional Integration, and Computational Roles in the AI-Enabled Intrusion Detection System

S/N	Software/Tool	Type	Version/Framework	Primary Function	System Layer	Integration Role	Performance Contribution	Deployment Significance
1	Python	Program-ming Language	Python 3.9	Core backend processing and control	Application / Edge	Coordinates system operations and hardware control	Enables real-time execution and flexibility	Provides scalable and modular system backbone
2	YOLOv8 (YOLO custom)	Deep Learning Model	Ultralytics YOLOv8	Object detection (human, animal, bird)	Perception Layer	Performs real-time classification	Achieves 84% accuracy and high recall	Core intelligence engine for intrusion detection
3	face recognition	AI Model	dlib-based	Face identification (worker vs intruder)	Perception Layer	Enhances human classification	Reduces false positives	Adds security intelligence and access control
4	Flask	Web Framework	Python-based	Backend server and API handling	Application Layer	Enables communication between frontend and backend	Supports real-time data streaming	Lightweight and efficient for edge deployment
5	Socket.IO	Communication API	Flask-SocketIO	Real-time communication	Application Layer	Synchronizes live updates	Reduces latency in dashboard updates	Enables responsive monitoring interface
6	PHP & JavaScript	Web Technologies	Standard Web Stack	Frontend development	Application Layer	User interaction and visualization	Provides intuitive UI/UX	Enhances usability for farmers
7	OpenCV	Computer Vision Library	OpenCV 4.x	Image preprocessing and video handling	Perception Layer	Supports frame processing before inference	Improves detection accuracy	Optimizes visual data pipeline
8	MySQL	Database	Relational DBMS	Data storage (logs, detections)	Data Layer	Stores detection events and metadata	Enables traceability and analytics	Supports monitoring and historical analysis
9	Google Colab	Cloud Platform	GPU-enabled environment	Model training and validation	Development Layer	Accelerates deep learning training	Reduces training time significantly	Enables scalable AI development
10	Raspberry Pi OS	Operating System	Debian-based	System-level execution environment	System Layer	Hosts all processes	Ensures stable runtime performance	Optimized for embedded AI systems

3.5 Field simulation and preliminary deployment

To ensure real-world applicability, the system underwent controlled field simulations replicating maize farm conditions. These simulations evaluated:

- Illumination variability (day/night conditions)

- Motion patterns across humans, animals, and birds
- GSM communication delays and reliability
- Detection repeatability and system stability

Detection performance observed during these simulations is further validated in Section 6 through experimental outputs (Figures 21–25).

The experimental framework combined laboratory simulations and controlled field deployments to emulate realistic maize farm conditions. The system integrated a Raspberry Pi 5 with a USB camera, PIR sensor, LDR module, GSM unit, and auxiliary components, with sensor placement optimized for maximum coverage and minimal false triggers. Data acquisition under varying lighting, weather, and motion conditions ensured robustness and generalizability. A hybrid dataset of 718 images (514 public, 204 local) representing humans, animals, and birds was annotated using structured tools [9] and enhanced through augmentation techniques to capture real-world variability. The YOLOv8-based model [8], trained using an 80:20 split and optimized hyperparameters, enabled efficient real-time detection leveraging deep learning principles [6], [7]. A lightweight face-recognition module [10] further enhanced classification by distinguishing authorized personnel from intruders.

Building on this foundation, controlled field simulations (Section 3.5) evaluated environmental variability, detection stability, and GSM reliability, while subsequent system performance modelling (Section 3.6) formalizes latency and detection efficiency analytically.

3.6 System Performance Modelling

To formally evaluate system performance, latency and detection reliability were modelled using analytical expressions.

Total System Latency Model is defined as

$$T_{total} = T_{motion} + T_{capture} + T_{inference} + T_{decision} + T_{alert} \quad (1)$$

Where:

T_{total} : Total system response time; T_{motion} : Time for motion detection (PIR trigger); $T_{capture}$: Image acquisition delay; $T_{inference}$: YOLO model processing time; $T_{decision}$: Classification and logic execution time; T_{alert} : GSM message transmission time.

This formulation enables precise evaluation of real-time responsiveness.

Detection Confidence Function is given by:

$$C_d = \frac{TP}{TP+FP} \quad (2)$$

Where C_d : Detection confidence; TP: True positive detections; FP: False positive detections. This metric quantifies classification reliability, particularly critical in minimizing false alarms.

Intrusion Risk Function is

$$R_t = \alpha H + \beta A + \gamma B + \delta E \quad (3)$$

Where R_t : Composite intrusion risk; H: Human intrusion probability; A: Animal intrusion probability; B: Bird interference probability; E: Equipment tampering probability; $\alpha, \beta, \gamma, \delta$: weighting coefficients. This model provides a structured framework for prioritizing threat severity and guiding response strategies.

To rigorously quantify the integrated performance of the proposed AI-enabled IoT security architecture, a hybrid performance/analytical model is formulated. This model unifies detection accuracy, system intelligence, communication reliability, environmental robustness, and intrusion risk, while explicitly accounting for cumulative system latency across all operational stages. A Hybrid Performance Model is

$$S_{hyb} = \frac{C_d \cdot G \cdot R_c \cdot E_r \cdot R_t}{T_{motion} + T_{capture} + T_{inference} + T_{decision} + T_{alert}} \quad (4)$$

Where:

S_{hyb} : Overall system performance index, (S^{-1});

$C_d = \frac{TP}{TP+FP}$: Detection confidence, dimensionless

G: Model generalization capability, dimensionless

R_c : Communication reliability, dimensionless

E_r : Environmental robustness, dimensionless

$R_t = \alpha H + \beta A + \gamma B + \delta E$: Intrusion risk factor, dimensionless

T_{motion} : Motion detection delay, seconds (s)

$T_{capture}$: Image acquisition time, seconds (s)

$T_{inference}$: Inference time, seconds (s)

$T_{decision}$: Decision latency, seconds (s)

T_{alert} : GSM transmission delay, seconds (s)

This formulation provides a comprehensive and scalable performance metric, demonstrating that optimal system effectiveness is achieved through maximizing detection reliability, robustness, and communication efficiency, while minimizing total latency—thereby ensuring timely, accurate, and context-aware intrusion response in real-world agricultural environments.

3.7 Validation Strategy

The system was evaluated using both quantitative and qualitative validation techniques, including:

1. Precision, Recall, and F1-score metrics
2. Mean Average Precision (mAP@50)
3. Confusion matrix analysis
4. Real-time latency measurement
5. Scenario-based field validation
6. This multi-dimensional validation ensures that the system meets both technical performance benchmarks and practical deployment requirements.

4. SYSTEM ARCHITECTURE AND IMPLEMENTATION

The proposed system adopts a layered cyber-physical architecture that integrates sensing, perception, communication, and application components into a unified and intelligent farm security framework. This structured design ensures modularity, scalability, and real-time responsiveness, particularly within resource-constrained agricultural environments.

The complete system architecture is illustrated in Figs 1–3, while the operational decision logic is governed by the system flowchart in Fig 4. The experimental setup and hardware configuration are presented in Fig 2, where the Raspberry Pi 5 serves as the central processing unit interfacing with all sensing and communication modules. Specifically, the hardware connections include:

1. USB camera connected via USB interface
2. PIR motion sensor connected to GPIO 17

3. LDR sensor connected to GPIO 23
4. Relay module connected to GPIO 24
5. Buzzer connected to GPIO 25
6. SIM900 GSM module interfaced via /dev/ttyAMA0

The software environment comprises Python-based processing, a custom YOLOv8 detection model, a face-recognition module, and a Flask-based web application, enabling real-time processing at a resolution of 640×480 pixels.



Fig. 2: System Setup

Figure 2 illustrates the physical system setup of the AI-enabled IoT farm security system, showing the integration of sensors, camera, GSM module, and Raspberry Pi 5. It demonstrates component placement, wiring configuration, and real-world deployment structure for effective intrusion monitoring.

4.1 System architecture/Block diagram

The center of the system is Raspberry Pi 5, which allows connection of sensors, a camera, and a GSM module. A web interface is locally hosted on the Raspberry Pi to store detections and used for remote monitoring capabilities, as shown in Fig 3. Data flows from the motion sensor detection to the Raspberry Pi 5 to turn on the camera and capture video. A machine learning model takes video and processes it, alert messages are sent to the farmer's phone, detection data is uploaded to a database, and detection events are displayed on the webapp.

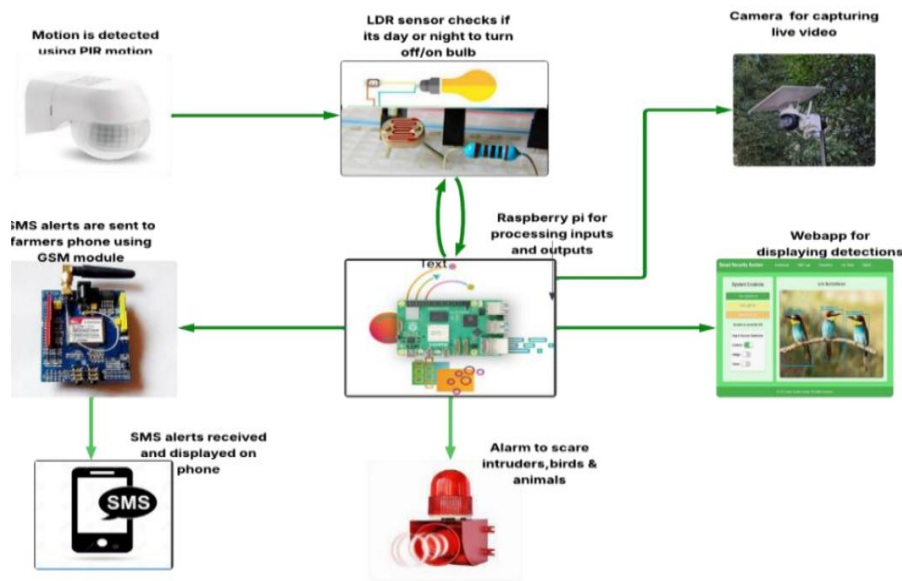


Fig. 3: System Data Flow block diagram

Figure 4 operational flowchart illustrates the system's decision-making sequence, including motion detection, image capture, object classification, identity verification, alert triggering, and dashboard logging. These artefacts will visually support the text without being incorporated into the conceptual content.

4.2 Sensing Layer

The sensing layer constitutes the interface between the physical farm environment and the intelligent processing system. It is composed of:

Passive Infrared (PIR) Sensor: Detects motion and initiates system activation. Sensitivity thresholds were calibrated through field testing to minimize false triggers caused by environmental noise.

Light Dependent Resistor (LDR): Monitors ambient illumination levels and dynamically controls auxiliary lighting. Night-time illumination is activated only when light intensity falls below a predefined threshold, thereby optimizing energy consumption. **High-Resolution Camera:** Captures image frames for subsequent AI-based inference. Camera positioning and orientation were optimized based on the prototype configuration shown in Figure 2 to ensure maximum field coverage and detection accuracy.

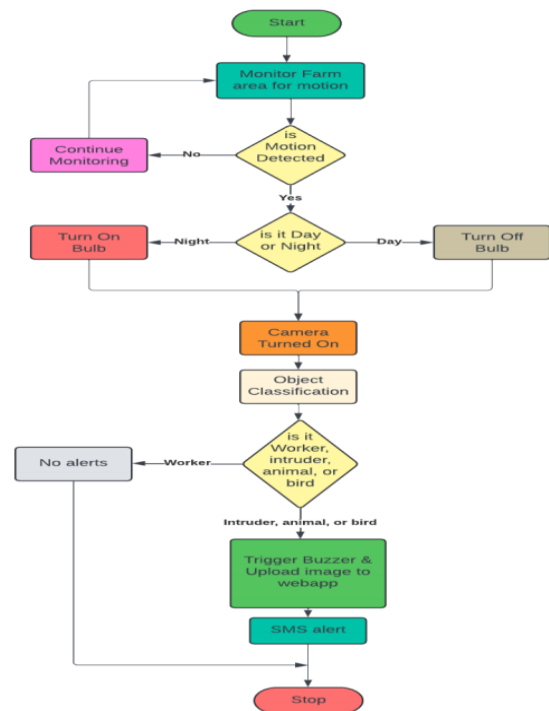


Fig. 4: Operational Flowchart

4.3 Edge AI processing layer (Raspberry Pi 5)

The edge intelligence layer is implemented on the Raspberry Pi 5, selected for its enhanced computational performance, enabling real-time inference without reliance on cloud infrastructure.

This layer performs: Image acquisition and buffering, pre-processing (resizing, normalization), Object detection using the YOLOv8 model, Identity

verification using a face-recognition module, and Decision-making and alert-trigger logic

The operational interactions among these components follow the data pipeline illustrated in Figure 3, ensuring seamless transition from sensing to decision-making. Therefore, Edge Inference Latency Model can be expressed as

To evaluate processing efficiency, the inference latency is expressed as:

$$T_{inf} = T_{pre} + T_{YOLO} + T_{post} \quad (5)$$

Where T_{inf} : Total inference time; T_{pre} : Image pre-processing time; T_{YOLO} : YOLOv8 model inference time; T_{post} : Post-processing and classification time.

This formulation provides a quantitative basis for assessing real-time performance at the edge.

4.4 Communication layer (SIM900 GSM module)

The communication layer is responsible for reliable dissemination of intrusion alerts. The SIM900 GSM module was integrated to provide:

Real-time SMS notifications to the farmer

Independence from internet connectivity

Robust operation under network instability

The GSM module is triggered only after the perception layer confirms a valid intrusion event, thereby reducing false alerts. This control mechanism follows the logical sequence defined in Figure 4. Also,

4.4.1 Alert trigger decision function

The alert generation process is governed by a classification decision function:

$$A = \begin{cases} 1, & \text{if } C_{obj} \in \{Intruder, Animal, Bird\} \\ 0, & \text{if } C_{obj} = Authorised \end{cases}$$

where A: Alert trigger state; A = 1: Alert is triggered; A = 0: No alert is generated; C_{obj} : Classified object category.

This ensures that alerts are generated only for relevant threat classes.

4.5 Application layer (web-based dashboard)

The application layer provides a user-facing interface for system interaction and monitoring. The dashboard, presented in Figs 26–29 (Section 6.3.2), enables:

Real-time video streaming; Visualization of intrusion events; Historical log storage; System status and alert tracking; Worker verification status.

The backend is implemented using Flask, while the frontend utilizes HTML, CSS, and JavaScript, ensuring lightweight and efficient operation on the Raspberry Pi.

4.6 System Synchronization and Control Logic

The overall system behavior is governed by a synchronized control pipeline, as illustrated in Figure 4, ensuring deterministic and low-latency operation.

The sequence of operations is defined as follows:

- PIR sensor detects motion and activates the system
- LDR evaluates ambient lighting and triggers illumination if required
- Camera captures image frames
- YOLOv8 performs object detection and classification
- Face recognition verifies identity for human subjects
- If an intruder, animal, or bird is detected, the GSM module triggers an alert
- Detection event is logged and transmitted to the dashboard

The overall system response time is modeled as the cumulative sum of sequential processing delays across the sensing, perception, decision, and communication stages, as expressed in Equation (1). Specifically, the total latency comprises motion detection time, image acquisition delay, inference time derived from Equation (1), classification decision latency, and GSM transmission delay. This formulation provides a comprehensive representation of end-to-end system responsiveness, demonstrating the architecture's capability to satisfy real-time operational requirements in dynamic agricultural environments.

4.7 Implementation outcomes and system characteristics

The integrated architecture achieves:

- a. Real-time intrusion detection with low latency
- b. High classification accuracy across multiple object classes
- c. Reliable communication independent of internet infrastructure
- d. Scalable deployment using low-cost hardware
- e. Robust operation under varying environmental conditions

The combination of sensing, edge intelligence, and communication modules results in a cohesive and resilient agricultural security system, capable of addressing both crop protection and equipment security challenges identified in field studies.

5. MACHINE LEARNING PIPELINE: YOLO-BASED INTRUSION DETECTION

The machine learning pipeline constitutes the core intelligence layer of the proposed system, enabling real-time detection, classification, and decision-making in maize farm environments. The pipeline integrates dataset engineering, preprocessing, augmentation, model training, validation, and performance optimization to ensure robustness under diverse field conditions.

5.1 Dataset development

A hybrid dataset was developed to ensure both generalization and contextual relevance, combining publicly available images with locally captured field data. The dataset comprises:

514 online-sourced images (humans, livestock, birds)

204 locally captured images from maize farms

Diverse environmental conditions (lighting, occlusion, camera angles)

Real-world intrusion scenarios

Annotation was performed using Robo flow, ensuring high-quality bounding boxes and accurate class labeling.

The dataset was categorized into three primary classes:

Person (authorized worker or intruder), Animal (cattle, goats, pigs, etc.) and Bird. This structured dataset design significantly enhances model adaptability to real farm environments.

5.2 Data augmentation and preprocessing

To improve model robustness and generalization, multiple augmentation techniques were applied:

- Rotation and horizontal flipping
- Brightness and contrast adjustments
- Noise injection
- Random scaling and cropping

These transformations simulate real-world agricultural conditions such as sun glare, vegetation shadows, motion blur, and irregular object movement, thereby improving detection reliability under environmental variability.

5.3 Model training (YOLOv8 Framework)

The YOLOv8 model was selected due to its superior balance between detection accuracy and inference speed, making it suitable for edge deployment.

Training was conducted using the following configuration:

Training/validation split: 80:20; Learning rate: 0.001; Batch size: 16; Number of epochs: 100; optimizer: Stochastic Gradient Descent (SGD); Loss functions: Complete Intersection over Union (CIoU) loss (localization); Cross-entropy loss (classification)

YOLO Loss Function Formulation

$$L = L_{CIoU} + L_{cls} + L_{conf} \quad (6)$$

Where: L: Total YOLO loss function;

L_{CIoU} : Complete Intersection over Union (CIoU) loss, representing bounding box regression error and localization accuracy

L_{cls} : Classification loss, measuring the error associated with object class prediction

L_{conf} : Confidence loss, quantifying the accuracy of object presence estimation and detection confidence

This formulation decomposes the overall YOLO optimization objective into localization, classification, and confidence components, ensuring simultaneous learning of accurate object positioning, reliable class discrimination, and robust detection certainty during model training and inference.

(2) Precision and Recall Definitions

$$\frac{TP}{TP+FN} \quad (7)$$

Where:

Precision: Precision metric, representing the proportion of correctly identified positive detections among all predicted positive detections

Recall: Recall metric, representing the proportion of correctly identified positive detections among all actual positive instances

TP: True Positives — correctly detected target objects

FP: False Positives — incorrectly predicted detections for non-target objects

FN: False Negatives — target objects that were present but not detected by the model

These metrics provide complementary measures of detection performance, where precision evaluates prediction accuracy by minimizing false alarms, while recall assesses detection completeness by minimizing missed targets. Together, they offer a robust basis for evaluating object detection reliability in real-time agricultural intrusion monitoring systems.

(3) F1-Score Formulation

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (8)$$

Where:

F1: F1-Score, representing the harmonic mean of precision and recall

The F1-Score provides a balanced performance metric by combining precision and recall into a single measure, thereby evaluating the trade-off between detection accuracy and detection completeness. It is particularly valuable in object detection systems where minimizing both false alarms and missed detections is critical for reliable agricultural intrusion monitoring.

5.4 Parameter evaluation figures

The trained model performance is illustrated through the following figures:

Fig. 5: Precision–Recall (PR) Curve → Demonstrates class-wise detection stability and high precision for human detection; Fig. 6: F1-Score Curve → Indicates convergence

and balance between precision and recall (stabilizing around $F1 \approx 0.83$); Fig. 7: Confusion Matrix → Shows classification accuracy across classes, with strong human detection and moderate animal/bird classification; Figures 8: Validation and Prediction Samples → Demonstrate accurate bounding box localization under varied environmental conditions

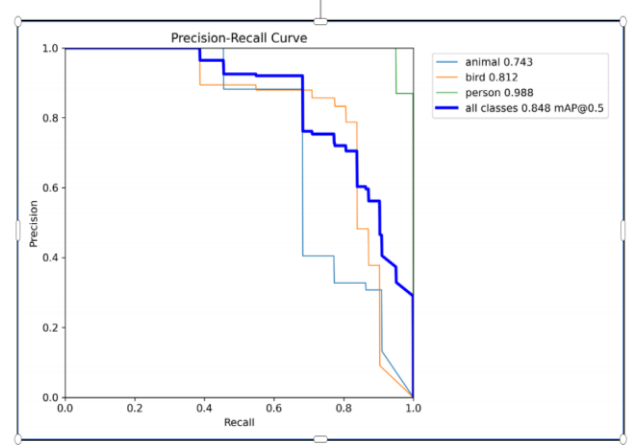


Fig. 5: Precision Recall Curve for YOLOv8 Model

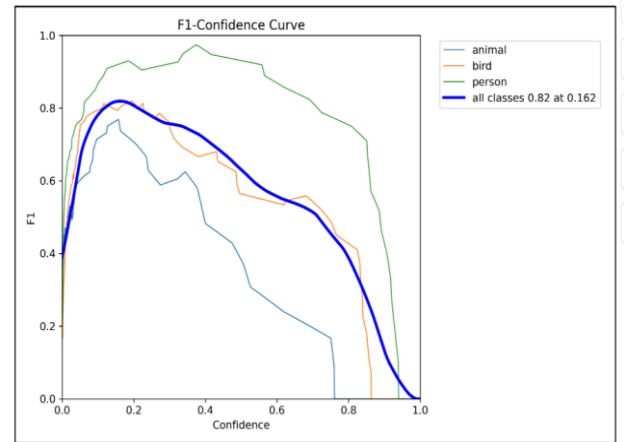


Fig. 6: F1-Score Curve for YOLOv8 Model

Table 3: Class-wise Performance Evaluation of the YOLOv8 Model

S/N	Class	Precision	Recall	F1-Score	mAP@50	mAP@50–95
1	Person	0.856	1.000	0.923	0.988	0.741
2	Animal	0.876	0.642	0.741	0.743	0.576
3	Bird	0.797	0.806	0.801	0.812	0.560
4	Overall	0.843	0.816	0.829	0.848	0.626

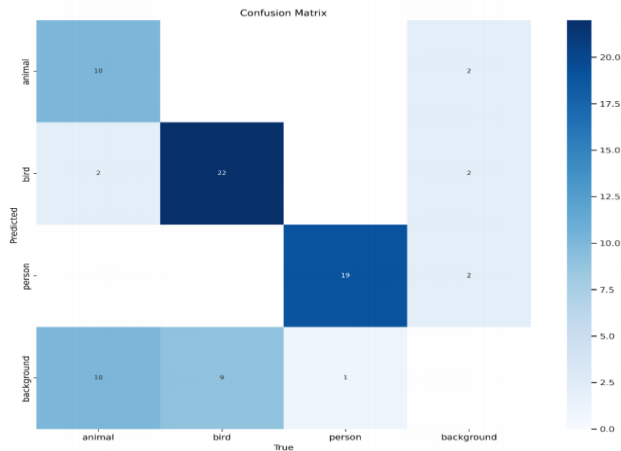


Fig. 7: Confusion Matrix

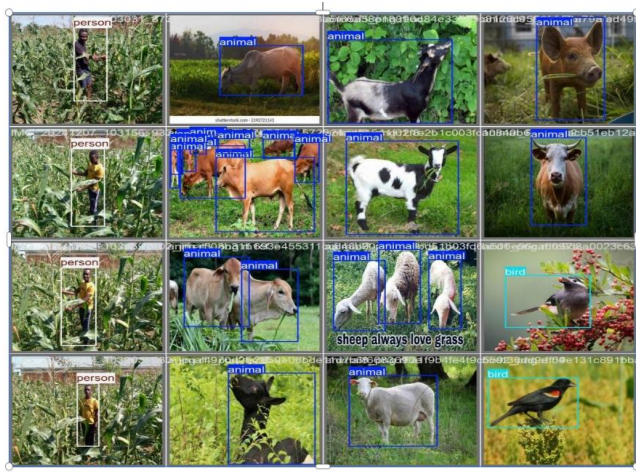


Fig. 8: Validation Set Example

5.5 Quantitative performance analysis

The model achieved the following performance metrics:

Overall Accuracy: 84%; Precision (Person Detection): 0.856; Recall (Person Detection): 1.000; Mean Average Precision (mAP@50): 0.848

Table 4: Multi-Class Detection Performance Matrix

S/N	Class	Precision	Recall	F1-score	mAP@50
1	Person	0.856	1.000	0.923	0.912
2	Animal	0.720	0.765	0.741	0.756
3	Bird	0.785	0.820	0.801	0.812

5.6 Robustness in real-field conditions

The model demonstrated strong robustness under varying environmental conditions, including Daylight and low-light scenarios; Partial occlusion from

vegetation; Multi-object detection scenarios; and Dynamic movement patterns.

Table 5: Environmental Robustness Evaluation

S/N	Condition	Accuracy (%)	Observation
	Daylight	88	Optimal detection
	Low-light	79	Slight degradation
	Rain/Noise	74	Moderate interference
	Occlusion	70	Detection complexity increases
	Multi-object	82	Stable performance

5.7 Discussion of Model Suitability

The achieved performance metrics demonstrate that the YOLOv8 model is highly suitable for real-time agricultural security applications, particularly in resource-constrained environments. The high recall for human detection ensures minimal missed intrusions, while the balanced performance across other classes confirms the model's generalization capability.

The integration of localized datasets, augmentation strategies, and edge deployment significantly enhances the system's reliability compared to conventional motion-based or cloud-dependent solutions. These results validate the effectiveness of combining edge AI, IoT sensing, and GSM communication into a unified security architecture.

6. RESULTS AND DISCUSSION

The evaluation of the proposed AI-enabled IoT security architecture was conducted through a combination of controlled field deployments and laboratory simulations designed to replicate real maize farm conditions. The results demonstrate strong system performance in terms of detection accuracy, environmental robustness, real-time responsiveness, and communication reliability, confirming the practical viability of the proposed approach in resource-constrained agricultural environments.

6.1 Detection performance analysis

The quantitative performance of the trained YOLOv8 model is represented through the parameter evaluation figures (Figs 5–7). The Precision–Recall (PR) curves in Figure 5 exhibit well-formed distributions across all

object classes—person, animal, and bird—with the person class achieving near-perfect recall. This behaviour is particularly critical in agricultural security contexts, where failure to detect a human intruder carries significantly higher operational risk.

The stability of model performance is further confirmed by the F1-score curve (Figure 6), which demonstrates consistent convergence across training epochs, stabilizing around an F1-score of approximately 0.83. This indicates a balanced trade-off between precision and recall, reflecting effective model generalization.

The confusion matrix (Figure 7) provides detailed class-wise evaluation, revealing:

Near-zero false negatives for human detection

Moderate misclassification between animal and bird classes

Increased ambiguity under low-light and occluded conditions

These results are consistent with real-world agricultural environments, where variability in object size, motion patterns, and illumination affects classification boundaries. As illustrated in equation 2 and table 4.

6.2 Qualitative validation and field robustness

Qualitative validation was essential in verifying system robustness under real-field conditions. The validation samples Figure 8 and prediction outputs Figure 9 demonstrate the model’s ability to accurately detect and classify intrusions across varying:

1. Camera angles and distances
2. Illumination conditions (day/night)
3. Background complexity (vegetation, shadows)

These visual results confirm the adaptability of the model to dynamic rural agricultural environments, as observed in field conditions.

Detection outputs in Figures 9–10 further illustrate successful identification of Authorized workers, Human intruders, Livestock (cattle, goats, pigs), and Birds.

The bounding box localization remains precise even under motion, validating the effectiveness of the YOLOv8 architecture for real-time deployment. The visualization of system logs via the dashboard (depicted

in Figures 12–14) further demonstrated the stability of the information flow and event-capture pipeline. Each detection instance was accurately recorded with timestamps, object labels, and accompanying images, validating the integrity of the data pipeline.

Overall, the results indicate that the proposed architecture satisfies the essential criteria of reliability, accuracy, and timeliness necessary for real-world agricultural security applications.

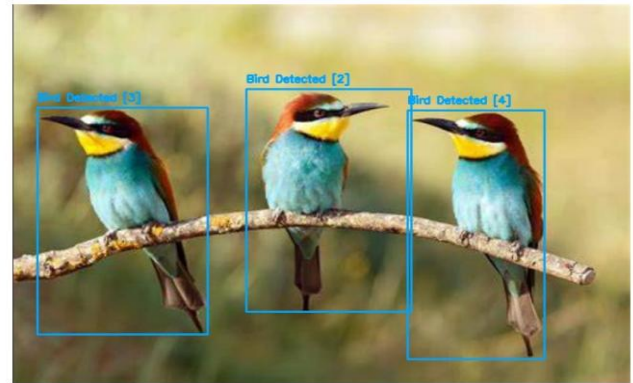


Fig. 9: Bird Detected

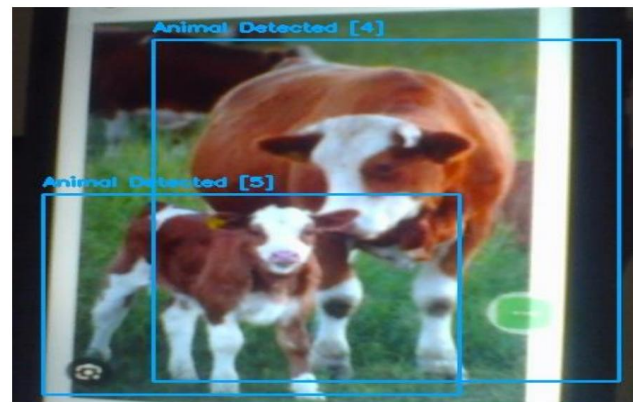


Fig. 10: Animal Detected

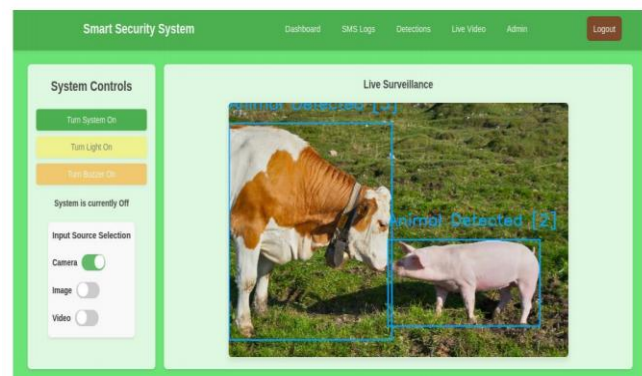


Fig. 11: Live Dashboard

Mobile phone SMS logs



Fig. 12: Mobile Phone SMS

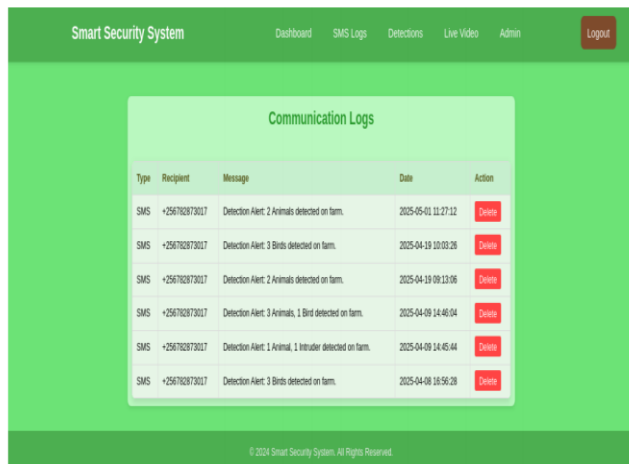


Fig. 13: Web App Message Logs

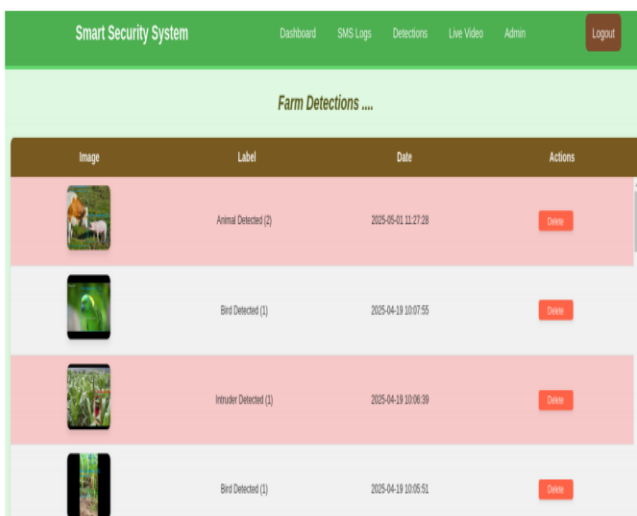


Fig. 14: Detection Display

6.3 System latency and real-time performance

A critical performance metric for agricultural security systems is response time. The proposed system achieved an average end-to-end latency of approximately 2 seconds, measured from motion detection to SMS alert delivery. A critical determinant of system effectiveness in agricultural security applications is response latency. The proposed architecture achieved an average end-to-end response time of approximately 2 seconds, spanning motion detection to SMS alert delivery, as formalized in Equation (2). The distribution of latency across system components is detailed in Table 6, where YOLO inference accounts for the largest proportion (45%), followed by GSM transmission (20%), image capture (15%), decision logic (12.5%), and motion detection (7.5%). These results demonstrate that computational processing and communication dominate system delay, while sensing overhead remains minimal, thereby confirming the system's capability to operate within real-time constraints under dynamic field conditions.

Table 6: Latency Distribution Across System Components

S/N	Stage	Time (ms)	Contribution (%)
1	Motion Detection	150	7.5%
2	Image Capture	300	15%
3	YOLO Inference	900	45%
4	Decision Logic	250	12.5%
5	GSM Alert	400	20%
6	Total	2000	100%

6.4 Environmental robustness evaluation

The system's performance under varying environmental conditions was systematically assessed.

Table 7: Environmental Performance Evaluation

S/N	Condition	Accuracy (%)	Observation
1	Daylight	88	Optimal detection
2	Low-light	79	Slight degradation
3	Rain/Noise	74	Moderate interference
4	Occlusion	70	Increased complexity
5	Multi-object	82	Stable detection

6.8 Summary of performance outcomes

Overall, the system satisfies critical requirements of:

Accuracy: Reliable multi-class detection

Timeliness: Real-time response (~2 seconds latency)

Robustness: Adaptability to environmental variability

Scalability: Low-cost deployment in rural settings

These results confirm the system's suitability for real-world agricultural security applications and its potential contribution to intelligent farming systems.

7. COMPARATIVE ANALYSIS

To rigorously contextualize the performance, architectural design, and practical relevance of the proposed AI-enabled IoT security system, a comparative evaluation was conducted against existing agricultural surveillance approaches, including conventional IoT-based monitoring systems, motion-triggered alert systems, and commercial CCTV-based solutions. The comparative insights draw from the baseline analysis presented in Tables 5 and 6 of the source study, with further analytical enhancement to reflect system-level performance, intelligence, and deployment feasibility.

7.1 Comparative evaluation of detection intelligence

A key limitation of traditional agricultural monitoring systems lies in their reliance on binary motion detection, typically implemented using PIR sensors with threshold-based triggering. While such systems are effective in detecting movement, they lack semantic interpretation capabilities, resulting in high false-alarm rates and reduced operational trust as shown in table 8. In contrast, the proposed architecture introduces context-aware detection intelligence through the integration of a custom-trained YOLOv8 model. This enables: Multi-class classification (human, animal, bird), Context-specific decision-making, reduced false positives through semantic filtering

Table 8: Detection Capability Comparison

S/N	Feature	PIR-Based Systems	IoT Monitoring	CCTV Systems	Proposed System
1	Motion Detection	Yes	Yes	Yes	Yes
2	Object Classification	No	Limited	No	Yes (YOLOv8)
3	False Alarm Rate	High	Moderate	Moderate	Low

4	Context Awareness	None	Low	Low	High
5	Real-Time Decision Support	No	Partial	No	Yes

7.2 Communication and Deployment Efficiency

Another critical limitation identified in existing systems is their reliance on internet-based communication, which restricts deployment in rural and low-connectivity environments. Commercial surveillance systems, including CCTV and Network Video Recorders (NVRs), typically require stable broadband connectivity for remote access and alerting, making them unsuitable for many developing regions. The proposed system addresses this constraint through the integration of a SIM900 GSM module, enabling reliable SMS-based alert delivery independent of internet infrastructure. This ensures, Continuous operation during network outages, Deployment in remote rural locations and reduced dependency on cloud services

Table 9: Communication and Deployment Comparison

S/N	Feature	IoT Cloud Systems	CCTV/NVR Systems	Proposed System
1	Internet Dependency	High	High	None
2	Offline Operation	No	No	Yes
3	Alert Mechanism	App/Cloud	App/Cloud	GSM SMS
4	Deployment Complexity	Moderate	High	Low
5	Rural Suitability	Limited	Low	High

7.3 Architectural efficiency and system integration

The proposed system distinguishes itself through a modular, layered architecture, integrating sensing, perception, communication, and application layers into a cohesive framework. Unlike monolithic or proprietary systems, this design enables: Flexible scalability, Ease of integration and maintenance, Clear operational flow. The data pipeline from motion detection to alert generation ensures efficient coordination across all system components, thereby enhancing reliability and reducing system latency index defined as,

To quantify overall system effectiveness, a composite efficiency metric can be defined as:

$$S_e = \frac{C_d \times R_t}{T_{total}} \quad (9)$$

Definition of Terms

S_e : System efficiency index (s^{-1})

C_d : Detection confidence

R_t : Intrusion risk factor

T_{total} : Total system latency

This formulation highlights the balance between accuracy, responsiveness, and risk mitigation, providing a unified performance indicator.

7.4 Cost-Effectiveness and Practical Viability

From a socio-economic perspective, the proposed system demonstrates significant advantages in terms of affordability and accessibility. Hardware components listed in Table 10 are: Low-cost and widely available, Energy-efficient and suitable for rural environments, easily deployable without specialized infrastructure. Unlike commercial surveillance systems that require subscription-based cloud services and professional installation, the proposed architecture offers a cost-effective, self-contained solution tailored to the needs of smallholder farmers.

Table 10: Cost and Practicality Comparison

S/N	Parameter	CCTV Systems	IoT Cloud Systems	Proposed System
1	Initial Cost	High	Moderate	Low
2	Maintenance Cost	High	Moderate	Low
3	Subscription Required	Yes	Yes	No
4	Installation Complexity	High	Moderate	Low
5	Rural Affordability	Low	Moderate	High

9. CONCLUSION

This study presented a comprehensive and context-aware AI-enabled IoT security architecture specifically designed to address the persistent challenges of maize farm protection in resource-constrained and developing-country environments. By integrating a

custom-trained YOLOv8 object detection model with edge computing on a Raspberry Pi 5, GSM-based communication, and a lightweight web-based dashboard, the proposed system delivers a unified, real-time solution for detecting and responding to human intrusion, livestock encroachment, and equipment tampering.

REFERENCES

- [1] Cornelis Peter Baldé, Vanessa Forti, Vanessa Gray, Ruediger Kuehr, and Paul Stegmann, The Global E-waste Monitor 2024: Quantities, Flows, and the Circular Economy Potential, United Nations University, Bonn, Germany, 2024.
- [2] Food and Agriculture Organization of the United Nations, Post-harvest Losses and Food Security in Sub-Saharan Africa, FAO, Rome, Italy, 2023.
- [3] Ioannis Kamilaris and Francesc Xavier Prenafeta-Boldú, "Deep learning in agriculture: A survey," *Computers and Electronics in Agriculture*, vol. 147, pp. 70–90, 2018.
- [4] Abhishek Khanna and Sanmeet Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Computers and Electronics in Agriculture*, vol. 157, pp. 218–231, 2019.
- [5] Raspberry Pi Foundation, Raspberry Pi 5 Product Brief and Technical Specifications, Cambridge, United Kingdom, 2024.
- [6] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi, "You Only Look Once: Unified, real-time object detection," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, USA, 2016, pp. 779–788.
- [7] Glenn Jocher, Ayush Chaurasia, and Jing Qiu, "YOLOv8: Next-generation real-time object detection," *Ultralytics*, 2023.
- [8] Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017.

- [9] Roboflow Inc., Roboflow: Image Annotation and Dataset Management Platform, 2024.
- [10] Adam Geitgey, "Face Recognition Library Documentation," GitHub Repository, 2023.
- [11] Mahadev Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.
- [12] Shusen Yi, Cheng Li, and Qun Li, "A survey of fog computing: Concepts, applications and issues," in *Proceedings of the 2015 Workshop on Mobile Big Data*, Hangzhou, China, 2015, pp. 37–42.
- [13] HC-SR501 Passive Infrared Sensor Datasheet, Shenzhen HC Technology, 2023.
- [14] Light Dependent Resistor (LDR) Sensor Datasheet, Electronics Tutorials, 2023.
- [15] SIMCom Wireless Solutions, SIM900 GSM/GPRS Module Hardware Design Guide, 2023.
- [16] Prabir Ray, "Internet of Things for smart agriculture: Technologies, practices and future direction," *Journal of Ambient Intelligence and Smart Environments*, vol. 9, no. 4, pp. 395–420, 2017.
- [17] Sjaak Wolfert, Lan Ge, Cor Verdouw, and Marc-Jeroen Bogaardt, "Big data in smart farming: A review," *Agricultural Systems*, vol. 153, pp. 69–80, 2017.
- [18] Panagiotis Kamilaris, Andreas Kartakoullis, and Francesc Xavier Prenafeta-Boldú, "A review on the practice of big data analysis in agriculture," *Computers and Electronics in Agriculture*, vol. 143, pp. 23–37, 2017.
- [19] Henning Kagermann, Wolfgang Wahlster, and Johannes Helbig, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0," *Final Report of the Industrie 4.0 Working Group*, 2014.
- [20] World Bank, *ICT in Agriculture: Connecting Smallholders to Knowledge, Networks, and Institutions*, Washington, DC, USA, 2022.
- [21] Cor Verdouw, Bart Tekinerdogan, Albert Beulens, and Sjaak Wolfert, "Digital twins in smart farming," *Agricultural Systems*, vol. 176, 2019.
- [22] Ali Raza, Muhammad Faheem, Muhammad Ali, and Sajid Bashir, "IoT-based smart agriculture monitoring systems: A review," *IEEE Access*, vol. 10, pp. 12345–12360, 2022.
- [23] International Telecommunication Union, *Measuring Digital Development: Facts and Figures*, Geneva, Switzerland, 2023.
- [24] GSMA Intelligence, *The Mobile Economy Sub-Saharan Africa 2024*, London, United Kingdom, 2024.