AgriCyber: AI- Driven Cybersecurity Framework for Soil Sensors and Irrigation Systems in Africa

Problem Statement

African agriculture increasingly relies on IoT devices, especially soil sensors (temperature, moisture) and smart irrigation systems to improve crop yields and manage scarce water resources. However, these systems operate in environments characterized by limited security controls, physical exposure, unreliable connectivity and high resource constraints, making them extremely vulnerable to data integrity attacks, particularly data spoofing and injection.

These attacks manipulate sensor readings on the devices, causing irrigation systems to behave incorrectly by overwatering, underwatering, or shutting down entirely, leading to severe crop losses for smallholder farmers who already operate on tight margins. These failures directly undermine **SDG 2: Zero Hunger**, as compromised irrigation systems reduce agricultural productivity, threaten food security and destabilize the livelihoods of millions who depend on farming.

Magnitude of the Problem: Agriculture & IoT in Africa

- Agriculture accounts for 25–35% of Africa's GDP and supports over 60% of the continent's workforce.
- Adoption of smart irrigation and soil-sensing systems is growing, especially in Kenya, South Africa, Nigeria, Morocco and Ghana.
- 80% of African farms are smallholder-owned, relying heavily on low-cost IoT devices with minimal built-in security.
- Intermittent internet and unreliable power force farmers to depend on edge-only, offline-capable devices, which are often the easiest to tamper with.

Why Focus on Soil Sensors + Smart Irrigation

- They are the most widely deployed IoT tools in African smallholder farms.
- They hold the greatest influence on crop health, water efficiency and yield outcomes.
- They are also the most vulnerable entry points due to poor hardware security, lack of encryption, and open-field deployment.
- A single spoofed moisture reading can destroy a full planting cycle, making this subset the highest-impact starting point for a cybersecurity and AI-driven protection framework.

Threat Landscape and African Contextual Challenges

While smart agriculture promises to close critical gaps in soil monitoring and irrigation efficiency, the African context presents a unique combination of cybersecurity, infrastructural, environmental, and socio-economic challenges that shape the threat landscape for any Agri-IoT deployment. Understanding these threats is essential, as the project will initially be rolled out in Africa, where the risks are both heightened and complex.

A. Cybersecurity Threat Landscape in African Agri-IoT Systems

1. **Weak or Non-existent Device Security**

Most low-cost soil sensors and irrigation controllers imported into African markets lack basic security capabilities such as:

- Encrypted communication,
- Secure firmware,
- Authenticated device identity, or
- Tamper-proof hardware.

Real Example:

In 2023, several East African agritech pilots reported incidents where counterfeit IoT soil probes were introduced into the supply chain, producing inaccurate moisture readings and causing irrigation system failures. These devices were traced to unauthorized distributors selling cloned hardware.

2**. Data Manipulation & False Data Injection**

Agricultural IoT systems are vulnerable to attackers or internal actors manipulating raw soil data to:

- Trigger wasteful irrigation cycles,
- Damage crops,
- Drive up energy costs, or
- Mislead analytics dashboards.

Real Example:

During a Nigerian smart-farm pilot in Oyo State (2022), inconsistent sensor readings were traced back to unauthorized configuration changes made by an on-site technician, highlighting how internal actors can pose risks in low-security environments.

3. Remote Takeover of Irrigation Systems

Weak remote-access controls in smart irrigation systems can allow attackers to:

- Turn pumps on/off,
- Drain water tanks,
- Sabotage crop cycles, or
- Overwork electrical components, leading to equipment burnout.

African Relevance:

Many farms rely on unprotected Wi-Fi or GSM controllers without firewalls or strong authentication, making remote takeover a realistic threat.

4. Supply-Chain Compromise

African markets often depend on imported IoT hardware from multiple suppliers. This creates risks such as:

- Unverified firmware,
- Tampered devices, or
- Inclusion of backdoors.

Real Example:

In Kenya (2021), counterfeit microcontrollers embedded in irrigation timers failed during the dry season, leading to crop losses. Later inspection showed they lacked OEM security signatures.

5. Denial-of-Service (DoS) from Connectivity Gaps

African farms frequently experience:

- Unstable mobile networks,
- Long periods with no connectivity, and
- Power outages.

Attackers could exploit these weak points to cause downtime or disrupt automated irrigation cycles.

Example:

Rural Ghana’s smart-farm pilots showed that even a 2–3 hour GSM outage caused crops to miss irrigation triggers, resulting in noticeable stress during the dry season.

6. Physical Tampering or Device Theft

IoT devices deployed in open farmlands are vulnerable to:

- Vandalism
- Theft for resale,
- Unauthorized adjustments, or
- Harvesting of components.

Example:

South African farms have reported theft of solar-powered irrigation controllers during power shortages, with devices resold in informal markets.

7. Low Digital Literacy & Trust Issues

Farmers may distrust automated systems or incorrectly operate them, increasing risks of:

- Misconfigured devices,
- Accidental system disablement, or
- Failure to update firmware.

Example:

In Uganda, farmers rejected a soil-sensor irrigation system after rumors spread that the devices were “monitoring their land for government acquisition.”

Trust is as important as technology.

B. African Environmental and Operational Challenges

1. Climate Variability and Unpredictable Rainfall

Africa is one of the regions most affected by climate change. Erratic rainfall compounds the need for accurate soil data and dynamic irrigation models.

Real Example:

The Horn of Africa drought (2020–2023) devastated smallholder farms that relied on calendar-based irrigation, proving the need for real-time data-driven practices.

2. Fragmented Water Infrastructure

Many farms lack:

- Reliable reservoirs,
- Stable pumping systems,
- Irrigation channels free of leakages.

Smart systems may trigger irrigation, but water may never reach the crop due to physical failures.

3. Limited Electricity and Battery Reliability

Soil sensors powered by batteries or solar may fail due to: low sunlight, battery theft, or low-cost power cells with short life cycles.

4. High Cost of Quality IoT Hardware

Most farmers rely on low-cost unverified hardware from informal markets because:

- certified hardware is too expensive,
- import taxes are high,
- maintenance services are scarce.

This increases vulnerability to cyber compromise and device failure.

5. Poor Regulatory Framework for IoT Security

Africa currently lacks comprehensive policies governing:

- IoT device certification,
- cybersecurity standards for agriculture,
- data ownership & ethical use in digital farming,
- secure supply-chain verification.

This leaves farmers unprotected from both cyber and commercial exploitation.

6. Limited Local Technical Expertise

Maintenance of smart irrigation systems often requires:

- advanced troubleshooting skills,
- knowledge of security protocols,
- firmware management,
- network diagnostics.

Many rural communities lack trained technicians, resulting in system downtime.

7. Socio-economic Vulnerability

Smallholder farmers—who form 70–80% of Africa's agricultural sector—operate on thin margins. Any system failure (whether cyber or physical) can cause:

- direct financial loss,
- food insecurity,
- reduced trust in technology.

Solution Overview and Framework Layer

This project presents an integrated three-layer ai-based cybersecurity framework specifically engineered for African agricultural IoT contexts. Our framework combines:

(1) Cybersecurity Layer- defense-in-depth strategies including TPM-secured gateways, end-to-end encryption and context-aware threat response playbooks.

(2) AI Detection Layer - machine learning-powered anomaly detection using autoencoders/isolation forest model/ (any model we use) and federated learning to identify data manipulation in real-time while preserving farmer privacy.

(3) Data Privacy & Governance Layer- farmer-centric data ownership models and region-appropriate policies. Unlike generic IoT security frameworks designed for other infrastructures, ours explicitly addresses African realities: intermittent connectivity, resource constraints, physical security vulnerabilities and cost sensitivity.

Focus Area

We strategically focus on soil sensors (measuring temperature, moisture) and smart irrigation systems as our domain and prioritize data spoofing and injection attacks as our primary threat vectors. This focused scope is intentional: rather than attempting to address all agricultural IoT threats superficially, we provide deep, actionable security for the most critical and widely-deployed systems in Africa. Our framework is designed as an extensible methodology that is a blueprint that can scale to other IoT applications (livestock monitoring, drone systems, supply chain tracking) and evolve as threat landscapes change.

Project Unique Selling Points:

African-Context Design

- Most IoT security frameworks assume reliable internet, adequate power and secure physical environments
- Our framework addresses:

- Poor connectivity: Edge AI processing, federated learning
- Resource constraints: Lightweight protocols, cost-effective solutions
- Physical tampering risks:TPM at gateway, defense against on-site attacks
- Limited technical expertise: Response playbooks tailored to local capacities

AI + Cybersecurity Integration

- Most solutions do either traditional cybersecurity or AI detection - not both in a cohesive system
- We integrate:
    - Cyber layer provides secure foundation (encryption, authentication, TPM)
    - AI layer adds intelligent detection (anomaly detection, adaptive learning)
    - They protect each other: Cyber defends against model poisoning; AI detects attacks cyber controls might miss

Focus on Soil Sensors + Smart Irrigation

- Focused on **highest-impact use case**: soil sensors + smart irrigation
    - Critical for food security (SDG 2)
    - Widely deployed in African agriculture
    - High vulnerability (data spoofing can destroy crops)

Privacy-First Design for Smallholder Farmers

- Our framework uses **federated learning** - data stays on farm, only model updates are shared
- Farmer **data ownership** is built into the framework .
- Appropriate for regions with evolving data protection laws.

Extensible Framework Methodology

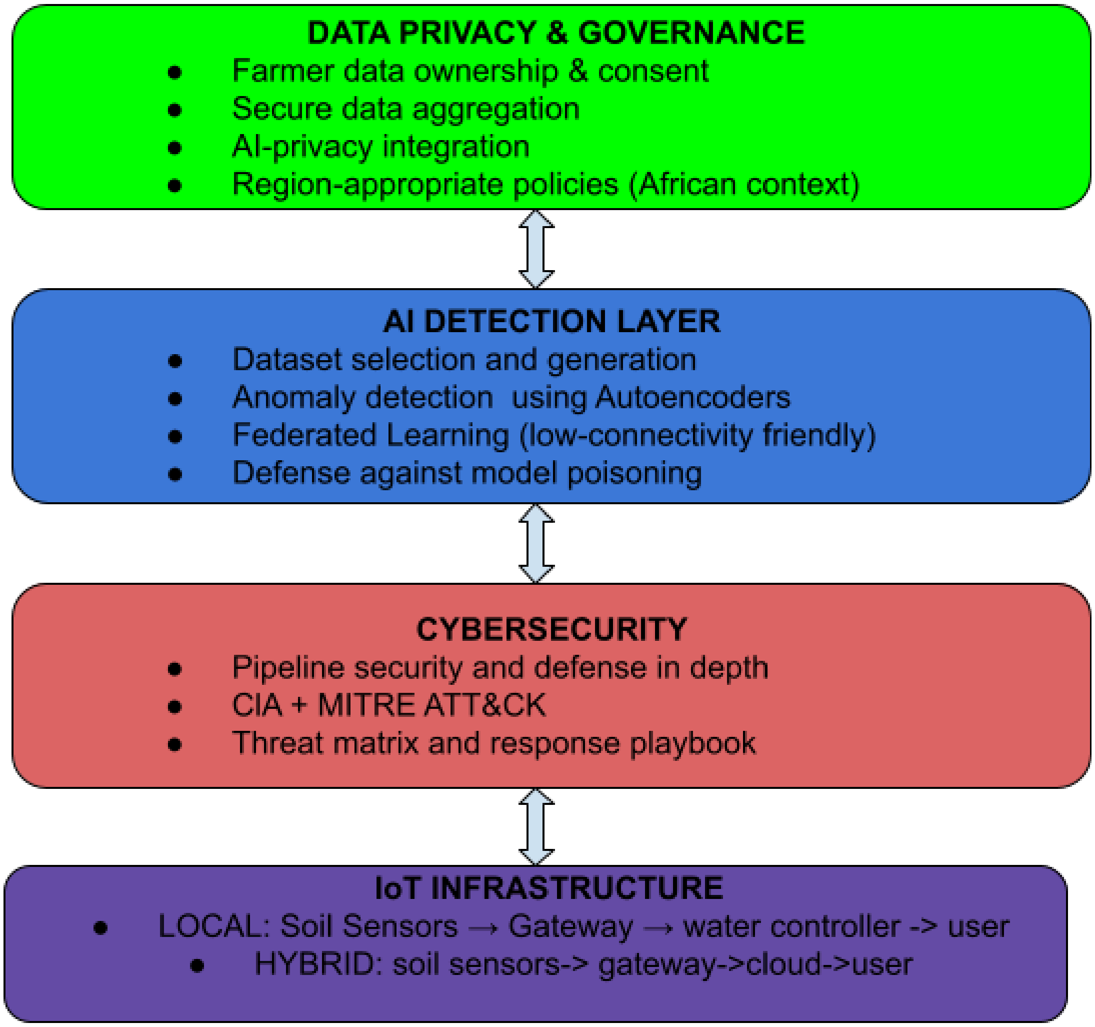
- It is not just a solution for one farm, it is a **replicable blueprint**
- Our framework can adapt to:
    - New IoT systems (livestock sensors, drones, supply chain)
    - Different African regions (varying infrastructure levels)

Project Objectives

1. **Detect sensor anomalies**
    - Identify data spoofing/injection in real time and flag sensor tampering using AI-enabled anomaly detection model(autoencoder).
    - Enable edge deployment for low-connectivity environments in Africa.

2. **Secure Data Pipeline**
    - Implement defense-in-depth from sensors to cloud
    - Protect data integrity, confidentiality and availability.
    - Design a lightweight and cost effective security control.

Framework Layers



DATA PRIVACY & GOVERNANCE

- Farmer data ownership & consent
- Secure data aggregation
- AI-privacy integration
- Region-appropriate policies (African context)

AI DETECTION LAYER

- Dataset selection and generation
- Anomaly detection using Autoencoders
- Federated Learning (low-connectivity friendly)
- Defense against model poisoning

CYBERSECURITY

- Pipeline security and defense in depth
- CIA + MITRE ATT&CK
- Threat matrix and response playbook

IoT INFRASTRUCTURE

- LOCAL: Soil Sensors → Gateway → water controller -> user
- HYBRID: soil sensors-> gateway->cloud->user

IOT INFRASTRUCTURE IN AFRICA

Local setting:

Sensors collect data → data sent to a local gateway/controller → gateway runs decision-making (model inference or rules) → gateway controls irrigation system directly → farmer sees results locally (e.g., local display, SMS).
No continuous internet needed.
Data and control fully on-premise.

Hybrid setting:
Same as local, but with intermittent cloud connectivity:
Gateway sometimes uploads stored data to cloud → cloud performs heavy model training/analytics → improved models or insights sent back to gateway or directly to farmer's remote apps → gateway continues local inference and control between cloud syncs.
Blends local autonomy + cloud learning and remote access.

Connection to SDG 2 - Zero hunger

Our framework contributes to SDG 2 through multiple reinforcing mechanisms:

- **Protecting Agricultural Productivity:** By preventing cyberattacks that cause irrigation failures, we safeguard crop yields that directly feed families and generate farmer income.
- **Water Resource Optimization:** Secure sensor data enables precision irrigation, reducing water waste by 30-50% while maintaining or increasing yields which is critical as climate change intensifies water scarcity.
- **Building Climate Resilience:** Reliable IoT helps farmers adapt irrigation to changing rainfall patterns, protecting food production against climate shocks.
- **Enabling Technology Adoption:** Addressing security concerns that inhibit IoT uptake, allowing more farmers to benefit from productivity-enhancing technology.
- **Protecting Farmer Livelihoods:** Preventing economic losses from cyberattacks that would push vulnerable farming households into deeper poverty and food insecurity.

➔ SECURE IoT FRAMEWORK
➔ PREVENTS DATA MANIPULATION
➔ RELIABLE IRRIGATION DECISIONS
➔ OPTIMIZED WATER USE + INCREASED YIELDS
➔ FOOD SECURITY FOR SMALLHOLDER FARMERS IN AFRICA
➔ SDG 2: ZERO HUNGER

Cybersecurity Defense-in-Depth Layer for AI-Driven Smart Irrigation IoT in Africa

1. Purpose and Scope

Smart agriculture systems rely on a continuous flow of data from ***sensors → gateway → cloud***. Because attackers can manipulate data at multiple points in this pipeline, a *defense-in-depth* approach is required. Although many threats exist, our focus is on ***data spoofing and injection, as they directly affect*** irrigation decisions and can cause significant crop loss.while considering

African agricultural realities such as intermittent connectivity, resource constraints, and physical vulnerabilities. This layer ensures ***confidentiality, integrity, and availability (CIA)*** of irrigation data, forming the foundation for AI-driven anomaly detection and privacy governance.

Physical Layer Security

In African agricultural environments, sensors and gateways are deployed in open fields with high physical exposure. Low-cost controls such as tamper-evident casings, secure device placement, and restricted access reduce the risk of malicious firmware installation or device replacement.

Research shows that low-cost agricultural IoT devices are highly vulnerable to physical tampering due to weak hardware protections (ENISA, 2017).

Layered Security Architecture

1. **Physical Layer**

- **Challenges**: Devices in open fields are vulnerable to tampering.
- **Controls**: Tamper-evident casings, secure placement, restricted access.

2. **Gateway Layer (Primary Focus)**

- **Risks**: Most likely attack point; enables MITM and data injection.
- **Controls**:
- **TPM**: Hardware-based identity and attestation.
- **Secure Boot + Signed Firmware**: Prevents unauthorized updates.
- **Mutual TLS (mTLS)**: Two-way authentication.
- **DTLS/MAC**: Lightweight integrity checks for rural networks.

3. **Sensor Layer**

- **Risks**: Physical spoofing and firmware tampering.
- **Controls**:
- Secure boot, lightweight authentication (e.g., DTLS over CoAP).
- Tamper-evident hardware.

4. **Cloud Layer**

- **Functions**: AI analytics, storage, model updates.
- **Controls**:
- **Blockchain Logging**: Immutable audit trails.
- **RBAC**: Least privilege access.

- **AES-256 Encryption**: Secure data storage.

Gateway Security (Primary Focus)

The gateway is the most realistic and impactful compromise point. A compromised gateway allows attackers to perform Man-in-the-Middle (MITM) attacks and inject falsified soil moisture data into the irrigation system.

Key Gateway Controls:

- **Trusted Platform Module (TPM):** Provides hardware-based identity, secure boot measurements, and cryptographic attestation.
- **Secure Boot + Signed Firmware:** Ensures the gateway only runs verified firmware, preventing unauthorized updates or malicious overwrites (CISA, 2023).
- **Mutual TLS (mTLS):** Enforces two-way authentication between the gateway and cloud to prevent spoofed devices or forged packets.
- **DTLS / Message Authentication Codes (MAC):** Lightweight cryptographic integrity checks suitable for low-bandwidth rural deployments.

These measures collectively block spoofed data packets, unauthorized firmware changes, and rogue network traffic.

MITRE ATT&CK / Cyber Kill Chain Mapping

- **Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Impact**
- Goal: Manipulate irrigation logic to cause overwatering or drought.

Context-Aware Threat Response

- Triggered by AI anomaly detection.
- Steps:

1. Verify sensor integrity via TPM.
2. Isolate compromised node.
3. Alert farmer via SMS/USSD.
4. Log event on blockchain.
5. Retrain AI model with new threat data.

Africa-Specific Adaptations

- **Lightweight Protocols**: CoAP + DTLS for low-power devices.
- **Offline Resilience**: Gateways operate autonomously during outages.
- **Cost Efficiency**: Open-source tools, affordable TPMs.
- **Farmer-Friendly**: Simple language, mobile alerts.

2. Pipeline Security Architecture

The IoT pipeline consists of three critical segments:

A. **Sensor Layer (Edge Devices)**
Soil moisture and temperature sensors deployed in open fields are highly vulnerable to physical tampering and spoofing attacks.
Controls:

- **Secure Boot & Firmware Integrity:** Sensors should implement cryptographic checks during startup to prevent unauthorized firmware changes.
- **Lightweight Authentication:** Use pre-shared keys or ECC-based lightweight protocols (e.g., DTLS over CoAP) for resource-constrained devices.
- **Tamper-Evident Hardware:** Physical seals or intrusion detection switches to alert gateways of tampering attempts.

B. **Gateway Layer (Field Gateway)**
Acts as the first aggregation point and security enforcement node.
Controls:

- **Trusted Platform Module (TPM):** Hardware-based root of trust for secure key storage and attestation.
- **End-to-End Encryption:** TLS 1.3 or DTLS for sensor-to-gateway and gateway-to-cloud communication.
- **Mutual Authentication:** Certificates or token-based authentication between gateway and cloud.
- **Local Threat Response:** Implement context-aware playbooks for isolation when spoofing is detected (e.g., block compromised sensor, switch to fallback irrigation schedule).

C. **Cloud Layer (Centralized or Regional Server)**
Provides advanced analytics, AI model updates, and long-term storage.
Controls:

  - **Blockchain-Based Logging:** Immutable logs for sensor readings and gateway actions to ensure integrity and traceability.
  - **Role-Based Access Control (RBAC):** Enforce least privilege for users and services.
  - **Data-at-Rest Encryption:** AES-256 for stored data; key rotation policies adapted to local compliance.

3. Defense-in-Depth Principles Applied

- **Physical Security:** Tamper-evident sensors, secure gateway enclosures, and farmer awareness training.
- **Network Security:** Segmentation between sensor network and management network; VPN tunnels for gateway-cloud communication.
- **Application Security:** Validate sensor data formats and ranges at multiple points to detect anomalies early.
- **Operational Security:** Regular patching schedules adapted to low-connectivity environments; offline update packages for gateways.

Cyber Defense Strategies (Defense-in-Depth)

Defense-in-Depth Approach

Purpose:
To create multiple layers of security so that if one fails, others still protect the system. This reduces the impact of threats like data spoofing, malware, and unauthorized access.

Key Security Layers

Layers	**Description**
Physical Security	Lock hardware, restrict access, use anti-tamper devices
Network Security	Firewalls, segmentation, VPNs, TLS encryption
Device & Endpoint	Authentication, certificates, secure firmware
Application Security	Input validation, API security, secure coding practices
Data Security	Encryption at rest/in transit, integrity checks (e.g., HMAC)
Monitoring & Detection	SIEM systems, anomaly detection, real-time alerts
Human/Process Layer	Training, access control policies, operational procedures

Incident Response Playbook: Spoofing Attack

A structured response plan to handle sensor data spoofing or gateway compromise.

1. **Detect**

- Alerts from abnormal sensor readings

- Suspicious firmware update attempts
- Integrity check failures (e.g., MAC/DTLS mismatch)

2. **Contain**

- Isolate gateway in its VLAN
- Revoke compromised certificates
- Block attacker IP or radio source

3. **Eradicate**

- Reflash gateway with signed firmware
- Verify integrity using TPM attestation
- Remove unauthorized scripts/binaries

4. **Recover**

- Re-issue device credentials
- Confirm sensor values normalize
- Restore irrigation schedules
- Document incident for future prevention

African Context Justification

These strategies are adapted to the realities of African agriculture:

- Devices are low-cost and often lack strong authentication
- Radio protocols may be unencrypted
- Monitoring infrastructure is limited
- Devices are physically exposed in open fields

Gateway-focused defense offers high impact at low cost.

Cybersecurity Playbooks: Why They Matter

What They Include:

- Threat description (e.g., spoofing)
- Detection steps (logs, alerts)
- Containment actions (isolate, block, revoke)
- Eradication steps (clean data, validate devices)
- Recovery steps (restore, re-authenticate)
- Post-incident review (root cause, lessons learned)

Benefits:

- Faster, consistent incident handling
- Fewer mistakes under pressure
- Clear roles and teamwork
- **Reflash gateway** with signed, validated firmware
- **Verify integrity** using TPM attestation
- **Remove unauthorized code** or binaries

B. Threat Modeling: Identifying What Can Go Wrong

Purpose:
To systematically identify vulnerabilities and anticipate how attackers might exploit them.

Methods Used

- **STRIDE**: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- **Attack Trees**: Visual maps of attacker paths
- **Data Flow Diagrams (DFDs)**: Highlight where data can be spoofed or injected

Threat Modeling Steps

1. **Identify Assets**: Sensors, cloud data, APIs
2. **Map Data Flow**: Sensor → Gateway → Cloud → Dashboard
3. **Identify Threats**: e.g., spoofing at sensor level
4. **Analyze Impact & Likelihood**
5. **Select Mitigations**: Authentication, encryption, validation, monitoring

Outcome:
A prioritized list of security controls based on real risk—not assumptions.

Focus Threat: Data Spoofing & Injection

What They Are:

- **Data Spoofing**: Fake data sent by a device pretending to be trusted
- **Data Injection**: Malicious data inserted or modified within the system

Defense-in-Depth Strategy

1. Physical Layer Security

- Lock and protect sensors

- Use tamper-evident seals
- Restrict access to gateways and equipment
- Use authentication labels or QR seals

Why?
Physical access enables direct data manipulation at the source.

2. Secure the Data Pipeline (End-to-End)

A. Sensor → Gateway

- Mutual authentication
- TLS/DTLS encryption
- Digital signatures on sensor data
- Whitelist trusted sensor IDs

B. Gateway → Cloud

- Secure API keys/certificates
- TLS tunnels or VPN
- HMAC for message integrity
- Cloud-side data validation

C. Cloud Processing & Storage

- Role-Based Access Control (RBAC)
- Logging and anomaly detection
- Protection against SQL/script injection
- Versioning and backups

3. Core Defense Techniques

- Strong device authentication (certs, tokens)
- Message integrity checks (HMAC, signatures)
- Sequence numbers/timestamps to detect replay
- AI-based anomaly detection
- Encrypted channels
- Input validation at all layers

Summary: Defense-in-Depth for Spoofing/Injection

Physical Layer	Secure sensors, lock hardware, tamper prevention
Sensor → Gateway	Encryption, mutual authentication, signed messages
Gateway → Cloud	Secure APIs, TLS, integrity checks, whitelisting

Cloud Layer	Identity verification, message integrity, abnormal data detection
Specific Threat	Identify verification, message integrity, abnormal data detection

Fit to African Context

- Response steps simple enough for non-technical smallholders
- Offline-first incident logging
- Low-cost controls (QR seals, ECC keys)
- Playbook supports community-shared security devices

Cybersecurity Layer: Threat Matrix & Spoofing Playbook

Threat Modeling: Data Spoofing & Injection + Mitigation Playbook

Threat Matrix (Focused on Data Spoofing & Injection)

Threat	Attack Vector	Impact	Mitigation
Sensor Data Spoofing	Physical tampering or fake sensor	Incorrect irrigation decisions	Tamper-evident seals, secure boot, anomaly detection
Data Injection via Gateway	Compromised gateway firmware	Corrupted aggregated data	TPM attestation, signed firmware updates
Man-in-the-Middle (MITM)	Intercepting sensor-gateway link	Data manipulation during transit	DTLS/TLS encryption, mutual authentication
Replay Attack	Reuse of old sensor readings	Misleading irrigation control	Nonce-based communication, timestamp validation

MITRE ATT\&CK / Cyber Kill Chain Mapping

- **Reconnaissance:** Adversary identifies exposed sensors in fields.
- **Weaponization:** Prepares spoofed sensor firmware or fake devices.
- **Delivery:** Physical access or network injection.
- **Exploitation:** Deploys malicious firmware or injects false readings.

- **Installation:** Establishes persistence on gateway or sensor.
- **Command & Control:** Sends crafted data to manipulate irrigation logic.
- **Actions on Objectives:** Causes over-irrigation or drought conditions, impacting crop yield.

Mitigation Mapped:

- Secure boot (stops rogue firmware)
- Signed packets (stops delivery/exploitation)
- TLS/DTLS (stops MITM)
- Anomaly detection (stops persistent spoofing)

Context-Aware Threat Response Playbook

Trigger: AI anomaly detection flags suspicious moisture readings inconsistent with historical patterns.

Steps:

1. **Verify Sensor Integrity:** Gateway checks TPM logs and sensor attestation.
2. **Isolate Compromised Node:** Block data from suspected sensor; switch irrigation to safe fallback mode.
3. **Alert Farmer:** Send SMS/USSD alert in local language for immediate action.
4. **Forensic Logging:** Record event in blockchain ledger for audit and compliance.
5. **Model Update:** AI layer retrains anomaly detection model with new threat signature.

Fit-to-Africa Considerations

- **Lightweight Protocols:** CoAP + DTLS for constrained devices.
- **Offline Resilience:** Gateways maintain local decision logic during connectivity outages.
- **Cost Sensitivity:** Use open-source cryptographic libraries and commodity TPM chips.
- **Human-Centric Design:** Playbooks use simple language and SMS alerts for farmers with limited technical literacy.

AI Layer

Dataset

This framework is designed to train the autoencoder for anomaly detection on sensor data collected from farms in regions across Africa. This is because different regions have unique patterns in rainfall, soil composition and prevalent crops like maize,beans,tomatoes and sorghum, making diverse regional data essential for robust model training.

However, for the purpose of demonstration, only synthetically generated data from a farm in Kenya has been used. following the detected sensor and farming patterns for this particular region.The dataset has 17000 readings assuming the farm is growing maize and tomatoes, The primary reference dataset is "Smart Farming Sensor Data for Yield Prediction" from Kaggle, which is an open-access resource containing typical agri-IoT measurements.

Real, complete and centralized IoT datasets covering all African crop types and farm conditions remain sparse The synthetic data points were generated to mimic:

- Soil moisture and temperature readings across real value ranges,
- Irrigation events and valve flow rates (in ml/min),
- Timestamp distribution,
- Crops
- Sensor IDs, to reflect actual device deployment,
- Patterns of sensor noise or missing readings (as commonly documented for low-cost hardware).

Limitations

- There is a significant challenge in aggregating real, large-scale, African IoT agricultural datasets into a central training corpus.
- Most available datasets are either fragmented or limited to specific experimental networks.

Model

Model Selection

- The model we have selected is the **autoencoder model.** It is suited for our use-case because of its ability to detect anomalies in soil sensors and water irrigation systems.
- The model is able to look at features in unison ie correlate features of the dataset eg. soil moisture , soil temperature and valve flow rates are correlated to detect anomalies.

- The model is great for low resource constraints because it can be adapted to be lightweight. Model inference can happen at the gateway without needing expensive servers or even cloud (hybrid settings can be used to intermittently do model training on local inexpensive server/cloud but to routinely use local gateways/devices for model inferences).
- The model is also suited for our medium-size dataset– check this

How Autoencoders detects anomalies

- Autoencoders are neural networks used for unsupervised learning of efficient, compressed representations of data.
- They consist of two main parts:
  - Encoder: Compresses (encodes) the input data into a smaller, abstract form known as the latent space or "bottleneck".
  - Decoder: Reconstructs the original input from this compressed representation, aiming to make the output as close to the input as possible.
- The "bottleneck" forces the network to learn the most important features and relationships within the data by limiting information flow.
- Since autoencoders get good at reconstructing data they have seen, the dataset needs to be containing clean and normal data. Abnormalities/anomalies in the dataset can train models to be insensitive to anomalies.

Model Training , Validation, Test and Inference

1)Training phase

- During training, the network learns what weights and parameters minimize the difference between the input and the reconstructed output (called the reconstruction error).
- The training stops when the reconstruction error reaches a convergence. That is, further iterations don't minimize the reconstruction error.

2)Validation Phase

- The trained model is evaluated on a separate validation set of clean, normal data (similar to the training set).
- Each validation sample is passed through the autoencoder, and its reconstruction error is calculated.
- The distribution of these errors is analyzed to set an anomaly detection threshold—typically at a high percentile (e.g., 99th) so most normal data falls below it.
- This threshold will be used to detect whether future samples are normal or anomalous.

3)Test Phase

- The model is tested on a new test set containing both normal and labeled anomalous samples.
- Each test sample's reconstruction error is computed and compared to the threshold.
- The model's performance is measured using metrics such as precision, recall, accuracy, and F1-score—indicating how well it detects true anomalies while minimizing false alarms.

4)Inference Phase (Real-World Use)

- The trained model is deployed to analyze incoming live data.
- For each new data sample, the reconstruction error is calculated.
- If the error is less than or equal to the threshold, the sample is considered normal.
- If the error exceeds the threshold, the sample is flagged as an anomaly for further investigation or response.

Summary of phases :

Phase	**Dataset Type**	**Contains Anomalies?**	**Purpose**
Train	Clean (normal)	No (ideally)	Learn what "normal" looks like
Validation	Clean (normal)	No (ideally)	Set the error threshold for anomaly
Test	Mixed (normal+anomaly)	Yes	Check precision/recall, F1, AUC
Inference	Live, real-world	Could have any	Detect anomalies in real time

Adaptations: Edge AI

Edge AI refers to the deployment of AI models directly on local edge devices or IoT-enabledIOT-enabled devices to enable real-time data processing and analysis without reliance on cloud servers. In the African agricultural context, this adaptation is vital for tackling resource constraints and safeguarding farmers' data privacy.

Edge AI for Resource Constraints and Data Privacy

- Most African smallholder farms operate with limited connectivity, intermittent power, and low-cost sensor hardware, making centralized cloud-based AI impractical and costly.
- Edge AI allows sensor devices or local controllers to process data in real-time and only send aggregated or anomaly alerts to the cloud, thus minimizing bandwidth needs and reducing reliance on external infrastructure.
- Edge AI enables precision farming by providing local, on-field detection and response to irregularities in sensor data such as soil moisture and temperature. For example, when the edge device detects a sudden drop in soil moisture, the anomaly detection model on the device can immediately activate irrigation valves to restore optimal conditions, all without involving any remote server or internet connection.
- Keeping sensor data local means sensitive information like farm IDsids, crop type and irrigation schedules is not continuously transmitted outside the farm, preserving farmers' privacy

Recommendation: Federated Learning

- To overcome the lack of central data that is highly needed to train and improve model performance, federated learning is recommended. This allows each farm to locally train an autoencoder model on its sensor streams (soil moisture, temperature) and irrigation data and to share only the model weights, not the raw data.

Federated Learning: What It Solves & CIA Triad

- Definition:
  Collaborative AI training where data remains on local devices; only model updates are shared and aggregated.
- What it solves:
  - Eliminates the need for central, full datasets.
  - Enhances scalability and inclusivity (many farms, devices, or organizations can participate).
  - Drastically improves privacy by keeping sensitive data local.

- CIA Triad Focus:
  - Primarily: Confidentiality
    - Raw data is never uploaded; only abstract model updates are shared.
    - Reduces risk of large-scale data breaches and privacy attacks.
  - Supports integrity and availability with robust protocols and redundancy, with C asIntegrity & Availability with robust protocols and redundancy, but C is the main focus.

Key Attack: Model Poisoning

- Threat:
  Malicious participants may send manipulated updates to the central server, aiming to corrupt the global model or introduce errors/backdoors.

Simple Mitigation Plan (DefenceDefense in Depth)

- People
  - Train operators in cybersecurity awareness.
  - Monitor for suspicious update patterns or false alerts.
- Process
  - Use incident response playbooks:
    - Detects anomalies in incoming model updates.
    - Isolate and investigate suspected sources.
    - Roll back global models if poisoning is detected.
- Technology
  - Robust model aggregation (median, trimmed mean) to limit the impact of any single update.
  - Validate model updates for outliers before accepting.
  - Authenticate clients; allow only trusted participants.
  - Use encrypted channels for all model communications (TLS/SSL).
  - Deploy cryptographic protocols (secure multiparty computation, homomorphic encryption) for additional protection.

Data Privacy and Governance Layer

1. Why Privacy Is Non-Negotiable

- Irrigation data reveals ownership, yield, water patterns, behaviors.

- Privacy protects farmers from exploitation and profiling.

- Ensures trust, legal compliance (NDPR, KDPA, POPIA), and safe Al use.

2. Privacy Governance Framework

- Secure Data Aggregation: encryption, mutual auth, minimized storage.

- Consent & Transparency: clear purpose, withdrawals allowed.

- Data Minimization: only essential sensor data used.

- Retention & Access Control: short retention, tiered access, audit logs.

3. Al-Privacy Integration

Federated Learning: data stays local; only model updates leave.

- Edge Al: reduces cloud dependency and lowers exposure.

- Differential Privacy: prevents reverse engineering of farm data.

- Privacy enforces limits: no raw datasets, privacy reviews for new inputs.

4. African Context

NDPR (Nigeria): consent, security, data subject rights.

- POPIA (South Africa): strict processing & security requirements.

-KDPA (Kenya): lawful processing, rights, international transfers.

- Rwanda/Uganda: emerging data protection bills. Offline consent, low-connectivity design, cooperative-friendly docs.

5. Responsibilities

- Approve Al datasets and ensure minimization.

- Define retention and deletion schedules.

- Draft consent frameworks and farmer rights guidelines.

- Review Al models for privacy compliance.

- Coordinate with Cybersecurity subgroup on shared risks.

6. Core Message

- Privacy rules everything:

• It controls what Al can learn.

• It defines how data flows.

• It ensures farmers remain owners of their data.

- Strong governance makes irrigation systems trustworthy and secure.

SDG CONTRIBUTION AND SOLUTION IMPACT

BENEFIT

- **Precision Agriculture**: Real-time sensor data enables targeted irrigation based on crop and soil needs.
- **AI Forecast Integration**: Machine learning improves weather prediction and irrigation timing.
- **Climate Adaptation**: Maintains soil moisture during droughts and heatwaves, boosting crop resilience.
- **Remote Monitoring**: Farmers control irrigation via smart devices, reducing labor and heat exposure.
- **Smart Farming Integration**: Combines irrigation with renewable energy (agrivoltaics), enhancing land-use efficiency.

STAKEHOLDER VALUE

1. **Smallholder Farmer Empowerment**

- **Smarter Decisions**: Real-time data on soil, weather, and crop needs improves irrigation choices.
- **Higher Yields & Lower Costs**: Efficient water use boosts productivity and reduces losses.
- **Data Protection**: Cybersecurity safeguards farm data, irrigation controls, and financial transactions.

2. **Rural Innovation Uptake**

- **Trusted Technology**: Cyber-secure systems encourage adoption and investment in agri-tech.
- **New Jobs & Skills**: Creates roles in IoT, cybersecurity, and digital farming support.
- **Community Growth**: Supports local markets, food programs, and cooperative farming networks

3. **Stakeholder Group:**

- **Agricultural cooperatives** - Better coordination, stronger bargaining power
- **Government & policy makers** - Reliable data for planning food security and water management
- **Agri-tech companies & startups** - Bigger market for secure IoT agriculture solutions
- **Financial institutions & insurers -** Lower risks when offering farm loans or crop insurance
- **Food supply chains & market**s - More reliable crop quantities and quality

EFFECTIVENESS: HIGHLIGHT ANY DEMO/TEST RESULTS & EFFICIENCY OF SOLUTIONS: Smart Drip Irrigation - International Journal of Research and Scientific Innovation (IJRSI)

Zimbabwe's farms are struggling with extreme heat and falling water levels, and in Region 2 over 70% of farmers depend on irrigation. The 2023 El Niño drought caused over 60% crop losses and is likely to worsen child nutrition by 2025. To help, a smart IoT irrigation system using soil-moisture sensors and the Blynk app was introduced so farmers can monitor and control watering in real time. This saves water, reduces labor, and improves crop health, making it a vital solution for drought-prone areas.

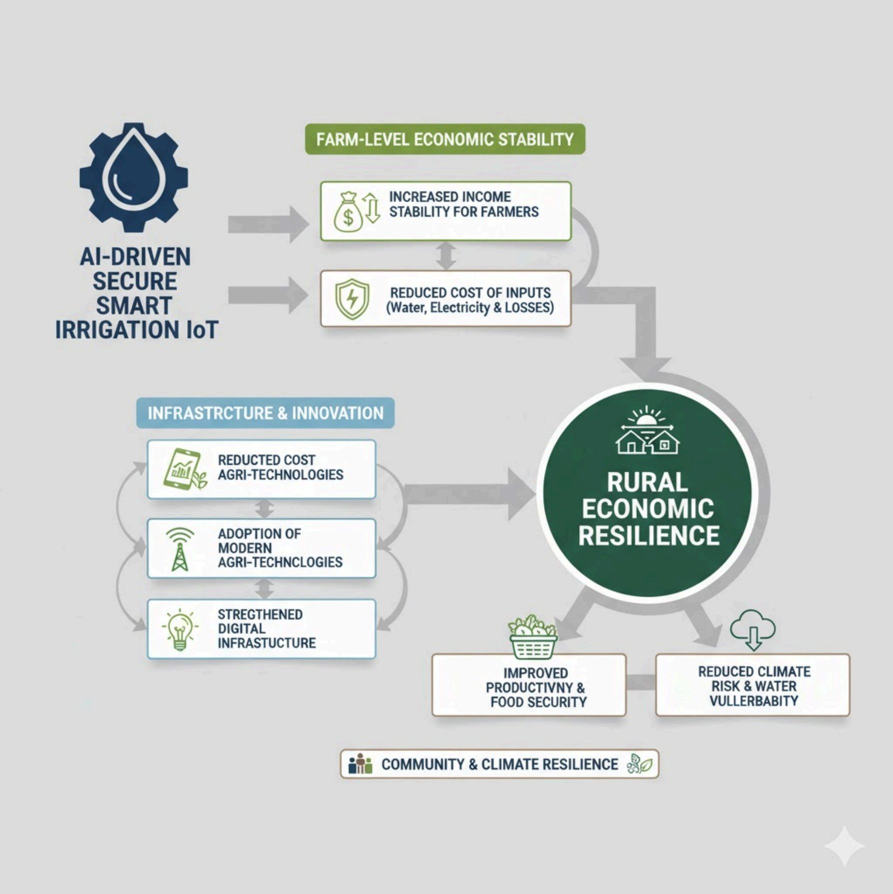
DESCRIPTION OF SDG 2 GOAL

- End hunger and malnutrition for all, especially vulnerable groups.
- Ensure year-round access to safe, nutritious, and sufficient food.
- Boost productivity and income for small-scale farmers, especially women and Indigenous communities.
- Promote sustainable agriculture and climate-resilient practices.
- Preserve genetic diversity of crops and livestock.
- Invest in rural infrastructure, research, and technology to enhance food systems.

Direct Pathways — how securing AI-IoT irrigation supports Zero Hunger

1. Secure sensors & actuators → Accurate irrigation control
2. Accurate control → Water savings + timely watering
3. Water savings + timely watering → Higher, more reliable yields
4. Reliable yields → More local food availability & stable incomes
5. Stable incomes → Greater household food security & investment in nutrition

Secure
IoT devices → Reliable data → AI decisions → Precise irrigation → ↑Yields & ↓Loss → Progress toward SDG2.


AI-DRIVEN SECURE SMART IRRIGATION IoT
FARM-LEVEL ECONOMIC STABILITY
INCREASED INCOME STABILITY FOR FARMERS
REDUCED COST OF INPUTS (Water, ELectricity & LOSSES)
INFRASTRCTURE & INNOVATION
REDUCTED COST AGRI-TECHNOLOGIES
ADOPTION OF MODERN AGRI-TECHNCLOGIES
STREGTHENED DIGITAL INFRASTUCTURE
RURAL ECONOMIC RESILIENCE
IMPROVED PRODUCTIVNY & FOOD SECURITY
REDUCED CLIMATE RISK & WATER VULLERBABITY
COMMUNITY & CLIMATE RESILIENCE

Key References

1. **Survey on Security Threats in Agricultural IoT**

   - Iera, A., et al. “Survey on Security Threats in Agricultural IoT and Smart Farming.” *Sensors*, vol. 20, no. 22, MDPI, 2020. (MDPI)

2. **Cybersecurity Challenges in Smart Agriculture**

   - Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. “Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven farms.” *World Journal of Advanced Research and Reviews*, 2022. (Wjarr)

3. **Trusted Computing Group — TPM and IoT**

   - Trusted Computing Group. “TCG Advocates Root of Trust, TPM and ICS Specifications for Protecting Internet of Things (IoT) Against Attacks.” TCG, 2013. (Trusted Computing Group)

   - Trusted Computing Group. “Internet of Things | Trusted Computing Group.” TCG. (Trusted Computing Group)

   - Trusted Computing Group. *Securing the IoT with Remote Device Attestation (TPM).* TCG technical booklet. (Trusted Computing Group)

4. **Federated Learning & Poisoning Attack Defenses**

   - Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A.-R. “Poisoning Attacks on Federated Learning-based IoT Intrusion Detection Systems.” NDSS Symposium, 2020. (NDSS Symposium)

   - Cao, X., Zhang, Z., Jia, J., & Gong, N. Z. “FLCert: Provably Secure Federated Learning against Poisoning Attacks.” arXiv, October 2022. (arXiv)

   - Hua, C., Yang, T., Sun, X., & Cui, Z. “Secure Hierarchical Federated Learning for Large-Scale AI Models: Poisoning Attack Defense and Privacy Preservation in AIoT.” *Electronics*, MDPI, 2025. (MDPI)

- “FedRecover: Recovering from Poisoning Attacks in Federated Learning using Historical Information.” arXiv, 2022. (arXiv)

5. **Poisoning in Federated Edge / IoT Learning**

   - Ferrag, M. A., Kantarci, B., Cordeiro, L. C., Debbah, M., & Choo, K.-K. R. “Poisoning Attacks in Federated Edge Learning for Digital Twin 6G-Enabled IoTs: An Anticipatory Study.” arXiv, 2023. (Studied impact on IoT federated systems.) (arXiv)

6. **Clean-Label Poisoning Attacks on IoT Federated Learning**

   - Yang, J., Zheng, J., Baker, T., Tang, S., Tan, Y., & Zhang, Q. “Clean-label poisoning attacks on federated learning for IoT.” *Expert Systems*, 2023. (NCHR)

7. **Robust Federated Learning Against Poisoning**

   - Electronics journal. “Robust Federated Learning Against Data Poisoning Attacks: Prevention and Detection of Attacked Nodes.” MDPI, 2025. (MDPI)