

2025

**Federal University of
Technology, Minna,
Nigeria**

NJTR



Nigerian Journal of Technological Research

Vol. 20, No. 2, December 2025



Production supported by:



- **AGRICULTURAL TECHNOLOGY**
- **EDUCATIONAL TECHNOLOGY**
- **ENGINEERING SCIENCES**
- **ENVIRONMENTAL TECHNOLOGY**
- **INNOVATION TECHNOLOGY**
- **INFORMATION AND
COMMUNICATION TECHNOLOGY**
- **LIFE SCIENCES**
- **PHYSICAL SCIENCES**

2025

**Federal University of
Technology, Minna,
Nigeria**



Nigerian Journal of Technological Research

Vol. 20, No. 2, Dec. 2025



Production Supported by



**TERTIARY EDUCATION TRUST FUND,
ABUJA, NIGERIA**

- **AGRICULTURAL TECHNOLOGY**
- **EDUCATIONAL TECHNOLOGY**
- **ENGINEERING SCIENCES**
- **ENVIRONMENTAL TECHNOLOGY**
- **INNOVATION TECHNOLOGY**
- **INFORMATION AND
COMMUNICATION TECHNOLOGY**
- **LIFE SCIENCES**
- **PHYSICAL SCIENCES**

NIGERIAN JOURNAL OF TECHNOLOGICAL RESEARCH

ISSN: 0795-5111
VOL. 20, NO. 2, DEC. 2025



Published by:

**FEDERAL UNIVERSITY OF
TECHNOLOGY, MINNA, NIGERIA.**

COPYRIGHT STATEMENT: The Nigerian Journal of Technological Research (NJTR), published by Federal University of Technology, Minna, Niger State, Nigeria is a fully Open Access journal committed to the principle that making research freely available to the public supports a greater global exchange of knowledge.

All articles published in the Nigerian Journal of Technological Research are distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

This license permits authors and users to share, copy, distribute, and adapt the material in any medium, or format, even for commercial purposes, provided that appropriate credit is given to the original author(s) and the source. Authors retain copyright to their work.

NIGERIAN JOURNAL OF TECHNOLOGICAL RESEARCH

General Information

Background Brief: The Nigerian Journal of Technological Research (NJTR) is the official journal of the Federal University of Technology, Minna, Niger State, Nigeria. It was first published in June 1989. It has since made significant strides in its efforts to provide an avenue for the dissemination of relevant, up-to-date research information in the core areas of discipline available at the University at inception; namely, Pure and Applied Sciences, Engineering Technology, Environmental Technology and Agricultural Technology.

Philosophy: As a strictly scientific and technological journal, it tends to provide information on problem-solving technology to its immediate environment and the international community.

Development: The Journal's responsiveness to the dynamic nature of research and development at the Federal University of Technology, Minna, and its environs has widened its scope of information dissemination to include, but is not limited to, Agricultural Technology, Environmental Technology, Engineering, Information and Communication Technology (ICT), Life Sciences, Physical Sciences, Educational Technology, and Innovation Technology. It has developed electronic communication procedures to ensure it can reach a larger community more quickly. It is anticipated that the Journal will contain scientific data providing up-to-date information for problem-solving in the identified areas of the University program.

Management: The Nigerian Journal of Technological Research has a unique management structure which enables it to carry out its functions promptly. This includes the Management Board, Editorial Board, Editorial Advisory Board, Regional Editors, Associate Editors, and a Business Manager. These groups bring their vast knowledge to the journal, ensuring its quality and reputation for academic output.

Finally, the Management Board and the Editorial Board of the Nigerian Journal of Technological Research firmly believe in the quality of information that will benefit mankind, and they are committed to ensuring the productivity and quality of information dissemination.

Editor-in-Chief

Professor O. O. Morenikeji
Department of Urban and Regional Planning
School of Environmental Technology
Federal University of Technology, Minna, Nigeria.

Deputy Editor-in-Chief

Professor Kasim U. Isah
Department of Physics
School of Physical Sciences
Federal University of Technology, Minna, Nigeria.

Editorial Board

- | | | | |
|-----|-------------------------------|---|----------------------|
| 1. | Prof. O. O. Morenikeji | - | Editor-in-Chief |
| 2. | Prof. Kasim U. Isah | - | Dep. Editor-in-Chief |
| 3. | Prof. Abdulkareem A. Saka | - | Member |
| 4. | Prof. Chiemela E. Chinma | - | Member |
| 5. | Prof. Hussaini A. Makun | - | Member |
| 6. | Prof. Abdulsalami S. Kovo | - | Member |
| 7. | Prof. B. A. Adegboye | - | Member |
| 8. | Prof. Jude T. Kur | - | Member |
| 9. | Prof. I. A. Diugwu | - | Member |
| 10. | Prof. A. I. Gambari | - | Member |
| 11. | Dr. Fatimah Jibril Abduldayan | - | Member |
| 12. | Prof. Richard Jimoh | - | Member |

Associate Editors

1. Dr. C. K. - Tedaam University of Technology and Applied Sciences, School of Chemical and Biochemical Sciences, Department of Applied Chemistry, Postal Box 24, Upper East, Navrongo, Ghana
2. Prof. Samson Oluwaseyi BADA - School of Chemical and Metallurgical Engineering, Wits University, Johannesburg, South Africa
3. Dr. Nnedinma Umeokafor - Faculty of Engineering and Science, University of Greenwich, UK
4. Prof. Daniel Ayuk Mbi Egbe - Institute of Polymetric Materials and Testing, Johannes Kepler University Linz, Austria
5. Prof. Oluwafemi Ayodeji Adebo – Department of Biotechnology and Food Technology, University of Johannesburg, South Africa
6. Prof. (Mrs.) Paola Fantazzini Department of Physics and Astronomy, University of Bologna, Italy
7. Prof. M. D. Magaji Agric UDUS – Department of Crop Science, Usmanu Dan Fodiyyo University, Sokoto
8. Dr. Pamela Abbott – Information School. Sheffield University, UK
9. Professor Adnan Akhuzada – College of Computing & IT, University of Doha for Science & Technology, Doha, Qatar
10. Prof. Agaji Iorshashe – Department of Computer Science, Joseph Sarwuan Tarka University, Makurdi

EDITORIAL COMMENTS

This edition of the Nigerian Journal of Technological Research is the second for the year 2025, which was a remarkable year for the Editorial Board. The large number of submissions and the quality of the manuscripts are a huge encouragement to us. The Board organised a retreat for academic and administrative staff including our reviewers and thesis supervisors on the ethical use of Artificial Intelligence in academic writing. The knowledge gained through the workshop was brought to bear on the selection of articles published in this edition.

This issue presents a collection of papers covering practical developments across computing, environmental health, engineering, agriculture, and library science. In the technical fields, the research includes deep learning frameworks for real-time multi-facial recognition, genetic algorithm optimization for electrical distribution networks, and the analysis of hybrid support materials for direct methanol fuel cells. Cybersecurity and data-driven modelling are addressed through hybrid anomaly-based intrusion detection systems, STRIDE threat modelling for smart farms, and the use of explainable machine learning to analyse urban land surface temperature drivers. Environmental and public health investigations focus on radon exposure risks in drinking water, thermal comfort in university housing, the prevalence of water-related diseases, and the financial impacts of flooding on rural rice farming. Agricultural and commercial operations are examined through comparisons of soil microbial populations, the profitability of sorghum-legume cropping systems, and the role of digital procurement in supply chain resilience. The volume concludes with institutional studies in library science, which look at collection development under open access policies, service delivery metrics, and the specific information needs of visually impaired students.

As usual, the Editorial Board is ever grateful to the University Management for the immense support and encouragement provided to them. Also, the Board is appreciative of the support of TETFUND. The financial assistance received consistently from the Tertiary Education Trust Fund (TETFUND) has enabled the Journal to adopt the Diamond Open Access Policy. Authors no longer pay the Article Processing Fee. We hope to sustain this policy as long as we continue to receive funding from TETFUND.

Table of Contents

1. RADIOLOGICAL RISK EVALUATION OF RADON EXPOSURE THROUGH INGESTION AND INHALATION PATHWAYS IN DRINKING WATER.....	1
Bello, I. A., Vatsa, M. A., Momoh, A. H., Sa'id, A., Ayodele, F. G., Abadunmi, T., & Tijjani, F. S.	
2. COMPARISON OF MICROBIAL POPULATION ON COMPOST, NON-COMPOST AND FERTILIZED SOILS IN GUSAU, ZAMFARA STATE.....	9
Nyandjou Yomi Marie Carole, Okoye Rosemary	
3. ASSESSMENT OF THERMAL COMFORT IN SELECTED FEMALE HOSTELS AT GIDAN-KWANO, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA, NIGERIA	21
Author Name: Musa Titus Dada	
4. DESIGN AND IMPLEMENTATION OF A REAL-TIME CYBER-AWARE MONITORING SYSTEM FOR SMART FARM NETWORKS USING STRIDE THREAT MODELLING.....	35
Ismaila Idris (ismi.idris@futminna.edu.ng), Francis Gideon Oghie (gideontech21@gmail.com)1, Andrew A Uduimoh (a.uduimoh@futminna.edu.ng)1, Anyaora Peter (p.anyaora@futminna.edu.ng)1, Ramat Imam Abba (mydearimam2005@gmail.com)2, Hadiza Yusuf (hyusuf@umich.edu)3	
5. DEVELOPMENT OF A HYBRID ANOMALY-BASED INTRUSION DETECTION SYSTEM USING AUTOENCODER AND ISOLATION FOREST	48
Somtochukwu Chinedu, Andrew A Uduimoh, Anyaora Peter, John K Alhassan, Hadiza Yusuf	
6. THE ROLE OF OPEN ACCESS RESOURCES IN SHAPING COLLECTION DEVELOPMENT POLICIES IN UNIVERSITY OF ABUJA LIBRARY, NIGERIA	61
Martha Tizhe, Fatimah Abubakar Sayyadi, Zakariyawu Abdullahi, & Jessica Achie Kakoushio	
7. DIGITAL PROCUREMENT TRANSFORMATION AND ITS IMPACT ON SUPPLY CHAIN RESILIENCE IN EMERGING ECONOMIES	75
Obieze, Ewere Success and Nwajei, Felix Liberty	
8. EFFECT OF FLOOD ON RURAL LIVELIHOOD STRATEGIES OF RICE FARMERS IN YOBE STATE, NIGERIA.....	92
Dawayo, A. S., Umar, A.J.	
9. A DIAGNOSTIC ANALYSIS OF LAND SURFACE TEMPERATURE DRIVERS IN KADUNA METROPOLIS USING STATISTICAL METHODS AND SHAP-BASED EXPLAINABLE MACHINE LEARNING	105
Jacob, R. J., Youngu, T. T., Azua, S., & Bununu, Y. A.	
10. PREVALENCE OF WATER-RELATED DISEASES IN AKURE METROPOLIS, NIGERIA: IMPLICATIONS FOR SUSTAINABLE URBAN WATER MANAGEMENT.....	127
ODEDIRAN Bukola Sunday	
	127

11. PERCEPTION OF LIBRARIANS ON SERVICE DELIVERY FOR CUSTOMER SATISFACTION IN PUBLIC UNIVERSITIES IN NORTH-CENTRAL NIGERIA	140
Dr. Isah Osimetha SEIDU	
12. INFORMATION NEEDS OF VISUALLY IMPAIRED STUDENTS IN ACADEMIC LIBRARIES IN KATSINA STATE	159
13. REAL-TIME MULTI-FACIAL RECOGNITION SYSTEM USING DEEP LEARNING TECHNIQUES.....	169
Ahmed Musa Iliyasu, Etemi Joshua Garba, Yusuf Musa Malgwi, Mamuda Francis Itanyi	
14. RELIABILITY ASSESSMENT AND GENETIC ALGORITHM-BASED OPTIMIZATION OF THE ETEKWURU DISTRIBUTION NETWORK USING ETAP	179
Otonye Ene Ojuka, Tekena Kashmony Bala, Peace Baridindum Biragbara	

DESIGN AND IMPLEMENTATION OF A REAL-TIME CYBER-AWARE MONITORING SYSTEM FOR SMART FARM NETWORKS USING STRIDE THREAT MODELLING

Ismaila Idris (ismi.idris@futminna.edu.ng), Francis Gideon Oghie (gideontech21@gmail.com)¹, Andrew A Uduimoh (a.uduimoh@futminna.edu.ng)¹, Anyaora Peter (p.anyaora@futminna.edu.ng)¹, Ramat Imam Abba (mydearimam2005@gmail.com)², Hadiza Yusuf (hyusuf@umich.edu)³

¹Cyber Security Department, Federal University of Technology Minna

²Cyber Security Department, Air Force Institute of Technology Kaduna

³Computer and Information Science, University of Michigan-Dearborn

Abstract

Agricultural systems are increasingly digitalised through the Internet of Things (IoT), enhancing productivity and precision while simultaneously heightening exposure to cyber threats. This paper presents the design and implementation of a real-time cyber-aware monitoring system for smart farm networks using the STRIDE threat-modelling framework. Unlike previous conceptual applications of STRIDE, each threat category—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege—was operationalised into executable detection rules within a hybrid anomaly detection engine. The system combines deterministic logic derived from STRIDE with an Isolation Forest model ($n_{\text{estimators}} = 200$, $\text{contamination} = 0.05$, $\text{max_samples} = 256$) to enable adaptive zero-day threat detection and automated quarantine of compromised MQTT nodes. Using the Mendeley Smart-Farm dataset comprising approximately 3,000 sensor readings of temperature, humidity, and soil moisture, real-time streaming experiments were conducted under a 70:15:15 split. The system achieved Accuracy = 0.96, Precision = 1.00, Recall = 0.91, F1-score = 0.95, with a mean Detection Latency of 0.55 seconds and mean Time-to-Quarantine of 0.87 seconds. The findings confirm that integrating STRIDE with real-time detection and containment enhances resilience, auditability, and adaptive security within precision agriculture IoT environments.

Keywords: Smart Agriculture, IoT, STRIDE, Cyber-Aware Monitoring, Isolation Forest, MQTT

1.0 Introduction

The current trend in smart solutions for farming has transformed agriculture into a data-intensive domain, with the Internet of Things (IoT) at its core. Networks of interconnected sensors and actuators now automate irrigation, fertilization, and crop monitoring with remarkable precision and efficiency (Bui et al., 2024; Campoverde-Molina & Luján-Mora, 2024). However, this same interconnectivity increases vulnerability to cyber threats stemming from insecure communication protocols, weak authentication mechanisms, and remote accessibility (Islam et al., 2021; Roy et al.,

2022; Afzal et al., 2021). Cyberattacks targeting such systems can disrupt operations, compromise data integrity, and undermine trust in digital agriculture infrastructures (Subhash et al., 2023; Adewusi et al., 2022b).

Traditional intrusion detection systems used in agricultural IoT environments are largely static and signature-based. While such systems are effective at recognising previously known attack patterns, they typically struggle to detect zero-day threats or evolving attack behaviours that deviate from predefined signatures. This limitation becomes more pronounced in dynamic agricultural environments where legitimate sensor readings naturally fluctuate due to

changing weather conditions, soil properties, and crop requirements. As a result, static IDS approaches may generate false alarms or fail to detect subtle malicious manipulations. In addition, many traditional IDS implementations rely on manual post-detection responses rather than automated containment mechanisms, which increases response time and limits scalability in distributed agricultural networks.

This study targets these limitations by designing a real-time monitoring and quarantine architecture, grounded in the STRIDE threat-modelling toolkit. Originally developed for software risk analysis but adapted here for IoT-based smart farming, STRIDE classifies threats as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. STRIDE was selected because it is a proactive and component-centric threat modelling framework that enables systematic identification of vulnerabilities before system deployment, which is particularly important for IoT environments requiring continuous and pre-emptive security evaluation (Liu & Wang, 2023; Tang & Chen, 2024). In contrast, other frameworks such as PASTA emphasise process-driven risk assessment workflows, while LINDDUN focuses primarily on privacy-related threat analysis rather than operational security enforcement in cyber-physical systems (Malik et al., 2021; Liu & Wang, 2023). Due to its structured categorisation of threats and direct mapping between threat classes and system components, STRIDE provides a lightweight yet practical framework for translating theoretical threat modelling into executable detection and mitigation mechanisms within IoT infrastructures.

The integration of STRIDE with the IF algorithm combines rule-based precision with data-driven adaptability. STRIDE deterministic logic identifies explicitly defined threats; on the contrary, the Isolation

Forest learns statistical boundaries of normal operation in order to detect deviations that may signify zero-day attacks. This hybrid synergy allows for prediction, detection, and containment of known and emerging anomalies, creating a balanced approach toward enhancing resilience in precision agriculture IoT networks.

The quarantine manager will then isolate the compromised MQTT sessions upon detection, log all related actions, and further notify administrators through an interactive dashboard. An integrated detection-response-audit workflow transforms STRIDE from a theoretical threat-modelling framework into a fully functional operational defence mechanism in agricultural IoT systems.

Key contributions of this work are:

- i. Converting STRIDE from a static design framework into an executable, rule-based detection layer for a live smart-farm network.
- ii. Developing a hybrid detection architecture that fuses rule-based and anomaly-based analysis to detect and mitigate zero-day attacks effectively.
- iii. Automating quarantine procedures to isolate compromised nodes in real time while maintaining consistent containment policies.

Accuracy, recall, and F1-score are metrics quantifying the performance of the system, while operational metrics such as latency, mean-time-to-quarantine, and false-isolation rate quantify the resiliency and efficiency of the whole system. These metrics establish a lightweight, reproducible cybersecurity monitoring framework for precision agriculture.

The rest of this paper is organized as follows. Section 2 reviews related work on IoT threat modeling and hybrid intrusion-detection systems in agriculture. Section 3 provides details on the system architecture, dataset, and detection methodology. Section 4 describes the experimental setup, evaluation

results, and comparative discussion. Section 5 draws conclusions and presents directions for adaptive and scalable implementations of the proposed framework.

2.0 Literature Review

The fast growth of IoT-based technologies in agriculture has encouraged broad research in cybersecurity frameworks that guarantee data integrity and network resilience. Available literature on the subject can be broadly grouped into two categories: (1) conceptual threat-modelling approaches that map vulnerabilities across interconnected agricultural IoT devices, and (2) hybrid or anomaly-based IDSs designed for evolving and zero-day attacks.

2.1 Threat Modelling in Agricultural IoT Devices

Most of the Ag-IoT threat-modelling studies depend on design-oriented frameworks for identifying the vulnerabilities in sensors, actuators, and communication pathways. Islam et al. (2021) have applied STRIDE in IoT-enabled smart homes and found its suitability in distributed device networks. Roy et al. (2022) extended this by applying STRIDE in smart solar systems and discovered cross-layer attack vectors in decentralized infrastructures. Al-Asif et al. (2021) proposed the first-ever STRIDE-based framework customized in precision agriculture. They mapped the threats and countermeasures systematically across sensor-actuator ecosystems. Recently, Subhash et al. (2023) generalized STRIDE for IoT ecosystems and established that it is efficient for structured risk assessment but suffers from limitations concerning real-time monitoring and adaptive detection.

Besides STRIDE, other threat modeling frameworks have been explored, such as PASTA (Process for Attack Simulation and Threat Analysis) and LINDDUN (privacy-

oriented threat modeling). Liu and Wang (2023) presented that the STRIDE will remain preferable in IoT contexts due to its lightweight structure and can directly link threats with control mechanisms. Malik et al. (2021) and Campoverde-Molina and Luján-Mora (2024) identified that the proactive nature of STRIDE allows continuous evaluation at system design time unlike the reactive posturing of PASTA or privacy-centric orientation of LINDDUN. However, despite these advantages, most implementations of STRIDE in agriculture remain conceptual—they either lack runtime enforcement or automatic mitigation components. Roy et al. (2023); Ouaisa & Ouaisa (2025)

Recent works have tried to bridge this theoretical–practical gap. Tang and Chen (2024) highlighted the need to integrate STRIDE into live IoT architectures, calling for adaptive threat models with embedded rule enforcement. Adewusi et al. (2022a) and Berguiga et al. (2023) also noted that integrating machine learning with STRIDE has the potential to enhance real-time threat visibility; however, the empirical results remain limited in the agricultural deployments. These studies together indicate the growing recognition of the adaptability of STRIDE but stress the absence of a fully operationalized implementation in Ag-IoT settings.

2.2 Hybrid and Anomaly-Based Intrusion Detection

Parallel to conceptual frameworks, another stream of research on hybrid IDS architectures combines rule-based and anomaly-based detection to enhance robustness against zero-day threats. Üstebay et al. (2025) presented a two-tier IDS incorporating ensemble decision trees with the Isolation Forest algorithm, which posted strong accuracy but moderate recall (0.30–0.62) on zero-day samples. Zahoor et al.

(2025) integrated Isolation Forest with One-Class SVM to improve anomaly detection on IoT datasets; however, their system remains diagnostic as it could only generate alerts but no automated responses. Hybrid frameworks for IoT networks have also been presented by Bui et al. (2023) and Yin and Zhou (2022), where they reported increased precision at the cost of high computational overhead on resource-constrained devices.

Complementary studies by Lata and Kumar (n.d.), Dhirani et al. (2021), and Zhang et al. (2023) further validate the fact that the integration of statistical learning models with deterministic rule engines enhances zero-day adaptability. These systems still remain highly dependent on post-detection manual intervention, though. Adewusi et al. (2022b) and Yadav and Prakash (2024) pointed out the lack of automatic mechanisms for containment as one critical limitation in the existing hybrid IDS models, especially in agricultural deployments, where the network nodes are geographically dispersed and need self-sustaining defense systems.

Despite these advances, there still remains a gap between theoretically grounded threat-modelling and operational cybersecurity in Ag-IoT ecosystems. Most existing IDS frameworks only produce alerts, without integrated containment or audit trails, while most STRIDE-based research has been confined to classification of risk without any live enforcement. The current paper remedies this dual lacuna through operationalizing STRIDE as an executable rule-based detection layer, fusing it with Isolation Forest for anomaly detection, and incorporating an

automated quarantine mechanism. This results in an integrated cyber-aware monitoring framework capable of real-time adversary activity detection, isolation, and logging, enhancing resilience and auditability within smart agricultural networks for the first time—a select few examples being Adewusi et al. (2022a) and Wang & Luo (2023).

3.0 Materials and Methods

3.1 System Architecture

The cyber-aware monitoring system was designed to work as a real-time, end-to-end solution to meet with the needs of data acquisition, threat analysis, auto-quarantine, and visualization of monitoring tasks on an interactive dashboard. The solution has five primary modules, with communication carried out through the MQTT protocol:

- i. **Sensor Simulator:** Generates real temperature, humidity, and soil moisture values to mimic the functioning of sensors used in smart farmland settings.
- ii. **Threat Injector:** Injects controlled malicious payloads that represent different STRIDE threat categories to test the responsiveness of the system to these threats.
- iii. **Hybrid Detector:** The rule-based engine employs the Isolation Forest model via a logical OR operator to carry out anomaly detection.
- iv. **Quarantine Manager:** Automates containment actions when node or MQTT topics are compromised.
- v. **Monitoring Dashboard:** Implemented in Streamlit and displays live sensor readings, notifications, and any quarantine actions.

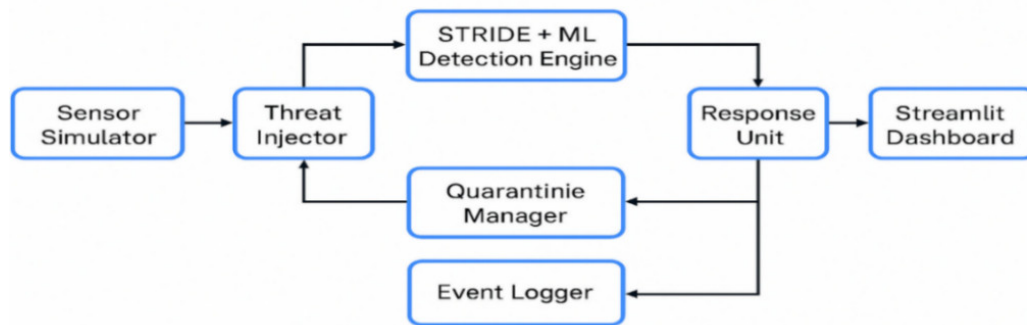


Figure 1: A modular diagram of the implementation framework highlights the important components (Figure created by the author).

3.2 Dataset

The experiment makes use of the Mendeley Smart-Farm Dataset, composed of real-world, compound time-series data of temperature, humidity, and soil moisture measured by IoT enabled sensors located in agricultural fields. The structured format of data makes it suitable for anomaly detection and real-time monitoring purposes. To simulating realistic network scenarios mimicking real-world publish-subscribe communication between agricultural node networks, data was transmitted through the MQTT protocol. The data was split evenly, with 70% used for training, 15% for validation and 15% for testing. The Isolation Forest model was trained on normal data, further optimized on the validation set, and finally validated with test data that included simulating adversarial data in accordance with the STRIDE threat models.

3.3 Detection Logic

The detection pipeline operates in two sequential analytical stages that combine deterministic rule evaluation with statistical anomaly analysis in order to identify both

predefined and previously unseen attack behaviours.

STRIDE Rule Engine: The rule engine implements executable detection conditions corresponding to each STRIDE threat category.

- i. Spoofing: Detection of abnormal authentication attempts or mismatched MQTT client identifiers indicating impersonation of legitimate nodes.
- ii. Tampering: Irregular variations in sensor payload values beyond expected operational thresholds.
- iii. Repudiation: Repeated or abrupt connection termination events suggesting attempts to deny or obscure prior actions.
- iv. Information Disclosure: Transmission of sensitive payload elements or credential patterns that may expose confidential information.
- v. Denial of Service: Excessive message publishing bursts from a single node exceeding normal communication rates.
- vi. Elevation of Privilege: Unauthorised control or configuration commands issued outside permitted operational roles.

Isolation Forest: The Isolation Forest model was applied to learn the normal bounds of

network traffic and give anomaly scores to new data points using only benign samples. The model was configured with 200 estimators, a contamination ratio of 0.05, and a maximum sample size of 256 per estimator. These parameters were selected to provide stable anomaly boundary learning while maintaining low computational overhead, which is important for real-time monitoring in resource-constrained IoT environments. On the feature set, temperature, humidity, and soil-moisture readings were considered for Min-Max scaling. We performed the training and evaluation in Python 3.12 using the scikit-learn library version 1.4.2 on a Windows 11 (64-bit) workstation driven by an Intel Core i7 (3.2 GHz) processor with 16 GB RAM. These parameters assured stable boundary learning, low computational overhead, and reliable anomaly detection performance during real-time MQTT stream monitoring in the smart-farm network.

Fusion Strategy: The results of both methods are combined with a logical OR operation. An event is considered malicious if it is either identified by one method or the other, thereby achieving maximum possible recall while maintaining acceptable precision.

Rationale for OR Fusion: The logical OR fusion was selected to prioritise detection coverage in safety-critical smart-farm environments, where missed attacks can directly disrupt irrigation, fertilisation, and environmental control processes. Under this strategy, a detection signal from either the STRIDE rule engine or the Isolation Forest triggers an alert, reducing the likelihood of false negatives when attack behaviour partially matches only one detection mechanism. In contrast, an AND-based fusion would require both subsystems to agree before raising an alert, which can improve precision but risks missing attacks that are detectable only by rules or only by anomaly patterns. Therefore, OR fusion provides a practical trade-off that favours

recall and early containment, aligning with real-time monitoring objectives.

3.4 Quarantine Manager

The quarantine component translates detection notifications into operational enforcement notifications. This takes place in one of two modes:

- i. *Shadow Mode:* Within the shadow mode, the suspicious MQTT clients are marked and recorded while not blocking them.
- ii. *Active Mode:* it instantly limits the right to publish or access the topic of any malicious entity that has been identified.

Every containment action is defined and controlled by a policy engine that operates with JSON-driven policies, while every operation is logged in an append-only audit log, which records information on timestamps, defining rules, affected resources, and performed actions.

3.5 Performance Metrics Calculation

System performance was evaluated through both detection metrics and operational efficiency metrics, derived from the model's confusion matrix. Let:

- i. **TP** = True Positives (attacks correctly detected)
- ii. **TN** = True Negatives (normal data correctly classified)
- iii. **FP** = False Positives (normal data incorrectly flagged as attack)
- iv. **FN** = False Negatives (attacks missed by the system)

The primary metrics were calculated as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1\text{-score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Latency (L): Measured as the mean time between message publication by the sensor and the corresponding detection decision:

$$L = \frac{1}{N} \sum_{i=1}^N (t_{d_i} - t_{p_i})$$

where t_{p_i} is the timestamp of message publication and t_{d_i} is the timestamp of detection.

Mean-Time-to-Quarantine (MTTQ):

Represents the average time between detection of an attack and execution of the quarantine action:

$$MTTQ = \frac{1}{M} \sum_{j=1}^M (t_{q_j} - t_{d_j})$$

where t_{d_j} is the detection timestamp and t_{q_j} is the quarantine timestamp.

False-Isolation Rate (FIR): Quantifies the proportion of benign nodes mistakenly quarantined:

$$FIR = \frac{FQ}{FQ + TQ}$$

where **FQ** is the number of false quarantines and **TQ** is the number of true quarantines.

Table 1: Detection Performance Across Configurations

Model	Accuracy	Precision	Recall	F1-score	Comment
Rule-Based (known threats)	1.00	1.00	1.00	1.00	Excellent for predefined patterns
Rule-Based (zero-day threats)	0.46	0.45	1.00	0.62	Fails on unseen behaviours
Isolation Forest (ML-only)	0.48	0.46	0.91	0.61	Detects anomalies but with moderate FP rate
Hybrid STRIDE + IF	0.96	1.00	0.91	0.95	Best overall performance

Throughput (T): Represents the average number of MQTT messages processed per second during live operation:

$$T = \frac{N_m}{t_{end} - t_{start}}$$

where N_m is the total number of messages processed and $t_{end} - t_{start}$ is the total observation duration.

4.0 Results and Discussion

4.1 Detection Engine Performance

The detection subsystem was experimentally evaluated under three configurations; rule-based, Isolation Forest (ML-only), and hybrid (STRIDE + IF), using controlled adversarial injection scenarios derived from STRIDE threat classes.

“Known threats” refer to attack patterns explicitly represented in the STRIDE rule engine (e.g., repeated login attempts, spoofed MQTT credentials, or tampering in sensor payloads).

“Zero-day threats” denote injected samples not covered by existing rules but generated by altering legitimate sensor values within statistically plausible limits ($\pm 25\%$ deviations in humidity or temperature, and $\pm 30\%$ in soil moisture), simulating unknown or mutated attack behaviours.

The dataset contained approximately 3,000 clean sensor readings representing temperature, humidity, and soil moisture data from the Mendeley Smart-Farm dataset. These readings were streamed through the sensor simulation layer to emulate live IoT activity. Within the threat injector layer, about 3,000 synthetic adversarial samples were introduced, distributed across STRIDE categories—spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

The hybrid model outperformed both standalone approaches because it combines deterministic rule precision with statistical generalisation. The STRIDE rule engine reliably captured predefined threat behaviours associated with authentication anomalies, message bursts, and abnormal command activity, while the Isolation Forest model identified deviations in sensor behaviour that were not explicitly encoded in the rule set. This complementary interaction explains the improved recall observed in the hybrid configuration when compared with rule-based detection alone.

Compared with related hybrid intrusion detection studies in IoT environments, similar behaviour has been reported where machine-learning components enhance adaptability while rule engines provide deterministic threat recognition. However, unlike several existing systems that only generate alerts, the proposed architecture integrates automated quarantine mechanisms, enabling immediate containment once an anomaly is confirmed. This integration strengthens operational cyber-awareness in smart agriculture networks.

Nevertheless, the observed performance should be interpreted with awareness of the experimental constraints. Because the evaluation relied on simulated threat injections, the anomaly patterns were generated under controlled conditions. Real-world adversarial behaviour may exhibit greater variability, which reinforces the importance of validating the proposed framework under diverse deployment environments.

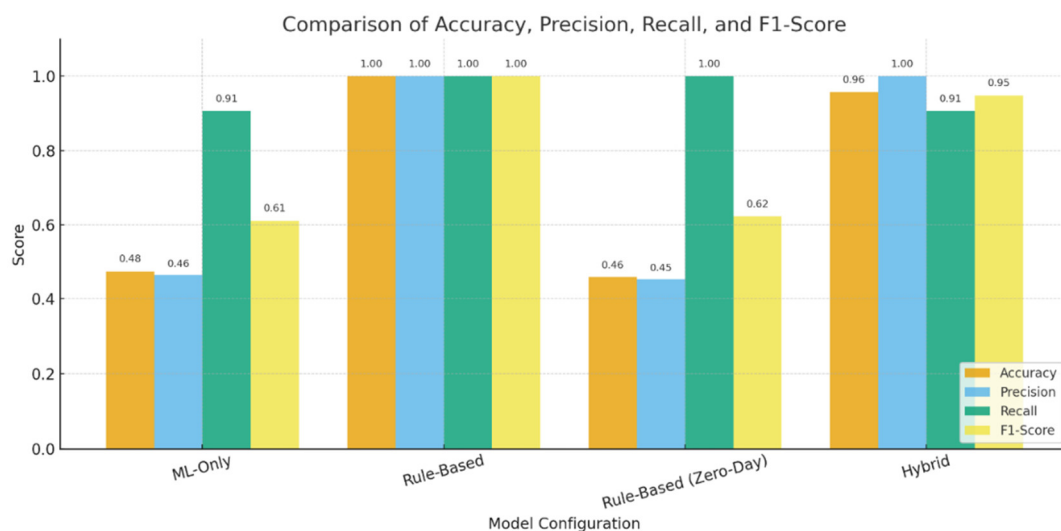


Figure 2 provides a visual representation of the evaluated Accuracy, Precision, Recall, and F1 scores for all three testing configurations.

Table 2 presents the confusion matrices summarising performance across

configurations. The matrices are based on a representative subset of the overall test data

to ensure clear visual presentation. Although the absolute counts were proportionally scaled, the derived performance ratios (Accuracy, Precision, Recall, and F1-score)

remain consistent with the results obtained on the full evaluation partition, which comprised approximately 450 samples (15 % of the 3 000-sample dataset).

Table 2. Confusion Matrices for All Configurations (Counts represent a proportionally scaled subset of the complete 3000-sample dataset; performance metrics were computed from the full evaluation results to maintain ratio consistency.)

Configuration	TN	FP	FN	TP
ML-Only	50	30	5	48
Rule-Based	80	0	0	53
Rule-Based (Zero-Day)	3	132	0	109
Hybrid (Final)	80	0	5	48

4.2 Quarantine and System KPIs

The quarantine manager executed isolation actions in both Shadow and Active modes, enforcing JSON-defined policy rules.

Performance monitoring via the psutil module confirmed CPU utilisation below 25% and memory consumption below 40% during live evaluation, showing its lightweight deployment suitability.

Table 3. System Operational Metrics

Metric	Measured Value	Interpretation
Detection Latency	0.55 s	Time between publication and alert generation
Mean-Time-to-Quarantine (MTTQ)	0.87 s	Average time from detection to isolation
False-Isolation Rate (FIR)	0.05	5% of benign nodes incorrectly quarantined
Throughput	1,850 messages/s	Sustainable load during real-time streaming

These operational results indicate that the proposed monitoring framework can provide practical security support for smart agricultural environments where IoT devices continuously exchange environmental and control data. In real farm deployments, environmental conditions such as weather changes, irrigation cycles, or sensor noise may naturally alter sensor readings. The

hybrid detection architecture helps maintain stability in such conditions because deterministic STRIDE rules capture explicit attack patterns while the anomaly detection component adapts to statistical deviations in sensor behaviour. Consequently, the framework can support continuous monitoring of distributed farm nodes while enabling rapid containment of suspicious activity.

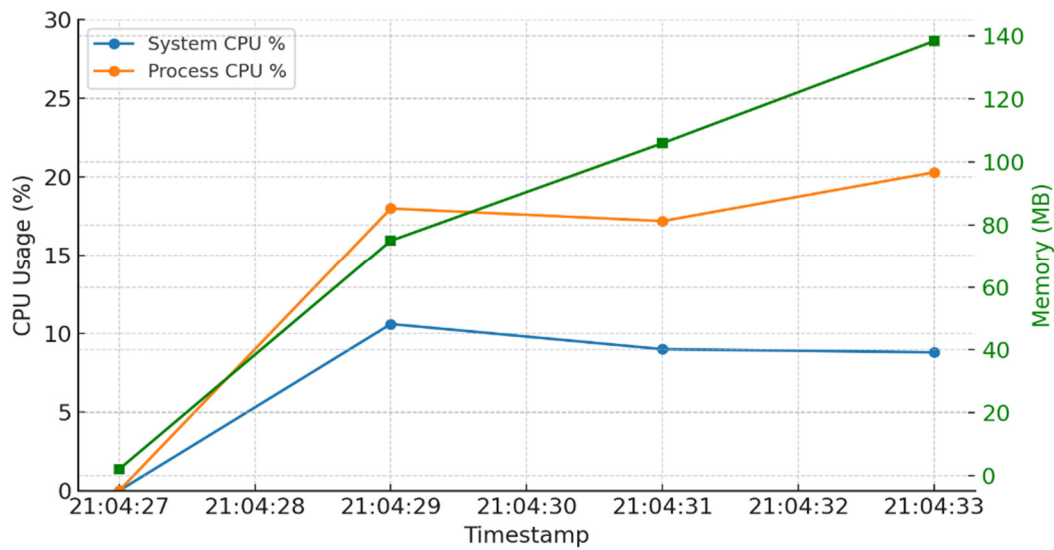


Figure 3: CPU and memory utilization of the detection engine during the simulation runs

4.3 Error Analysis

False positives were primarily caused by temporary fluctuations in sensor data, particularly humidity spikes, that mimicked tampering behaviour. False negatives occurred in rare cases where gradual attack patterns evolved too slowly to exceed Isolation Forest thresholds. Fine-tuning contamination rates or incorporating adaptive rule learning may further reduce these edge-case errors.

4.4 Comparative Analysis

To establish the value of the real-time STRIDE-based cyber-aware monitoring system, the findings were compared against two important reference studies:

Al Asif et al. (2021): a concept-level STRIDE threat-modelling framework for IoT-enabled agriculture studying some vulnerabilities and not offering enforcement or runtime validation.

Üstebay et al. (2025): a performance-driven IDS applying ensemble machine-learning models to IoT networks without STRIDE-based contextual mapping or automated response mechanisms.

The study operationalises STRIDE by merging a deterministic rule engine with anomaly detection and quarantine enforcement, thereby closing the gap between theoretical threat modelling and actionable IoT defence.

Table 4. Quantitative Comparison of IDS Models

Study	Accuracy	Precision	Recall	F1-score
Al Asif et al. (2021)	—	—	—	—
Üstebay et al. (2025)	0.98	0.97	0.55	0.64
Present Work (2025)	0.94	0.97	0.91	0.94

Table 5. Qualitative Characteristics of Compared Studies

Study	Approach / Focus	Key Contribution	Main Limitation
Al Asif et al. (2021)	Conceptual STRIDE model for Ag-IoT	Defined STRIDE threat map	No implementation
Üstebay et al. (2025)	Ensemble Tree + IF IDS	Multi-dataset benchmark	Weak zero-day recall; no mitigation
Present Work (2025)	STRIDE + IF Hybrid + Quarantine	Real-time detection + isolation	Single dataset; synthetic threats

The results indicate that integrating STRIDE-based deterministic rules with Isolation Forest anomaly detection improves overall detection performance within the evaluated smart-farm environment. The rule engine effectively identifies predefined attack behaviours associated with STRIDE threat categories, while the Isolation Forest model captures statistical deviations from normal sensor activity, thereby enabling detection of previously unseen or modified attack patterns.

The robustness of the system should be interpreted within the scope of the experimental design. The evaluation relied on the Mendeley Smart-Farm dataset and controlled STRIDE-based threat injections, which allowed reproducible testing of the detection pipeline but may not fully represent the diversity of real-world agricultural IoT deployments. Consequently, the findings demonstrate the effectiveness of the proposed architecture under simulated adversarial conditions while indicating the need for future validation across multiple datasets and real operational environments.

However, several limitations should be acknowledged. The evaluation was conducted using the Mendeley Smart-Farm dataset, which represents a specific agricultural sensing scenario and may not fully capture the diversity of device configurations, communication protocols, and operational conditions present across different agricultural IoT deployments. In

addition, the adversarial samples used in the experiments were generated through controlled STRIDE-based threat injections. Although this approach enables systematic and reproducible evaluation of the detection pipeline, it may not completely reflect the complexity and unpredictability of real-world cyber-attacks. Consequently, the reported performance should be interpreted as demonstrating the effectiveness of the proposed architecture within the experimental environment rather than as universal performance across all Ag-IoT infrastructures. Future studies should therefore extend validation using multiple datasets, heterogeneous IoT protocols, and real-world field deployments.

5.0 Conclusion

This study presented a real-time cyber-aware monitoring system for smart-farm IoT networks based on the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privileges) threat-modelling framework. The system translated each of the six STRIDE threat types into executable logics to constantly recognize and react to each threat in real time. The solution included a hybrid engine designed to detect threats in real time with deterministic rules centered on STRIDE and the Isolation Forest algorithm, which was known for high precision and recall in identifying known and zero-day attacks. The solution was further characterized by an

automated quarantine manager to isolate nodes that would not take action on anomalous traffic in addition to real-time visualization through the Streamlit dashboard.

Several directions can further strengthen the proposed framework. First, future studies should evaluate the system across multiple agricultural IoT datasets and communication protocols to assess scalability in heterogeneous environments. Second, practical deployment challenges such as network latency, edge-device processing constraints, and integration with farm management platforms should be investigated through field-scale pilot implementations. Third, long-term system adaptation could be enhanced through adaptive rule evolution, where STRIDE-based detection rules are periodically updated using threat intelligence and operational monitoring data. These developments would support the transition of the framework from a prototype monitoring system to a scalable and resilient cybersecurity solution for large-scale precision agriculture deployments.

Together, they represent the framework for transitioning this prototype to a self-adaptive and cyber-resilient monitoring framework for next-generation precision agriculture networks.

References

- Adewusi, A. O., Okechukwu, O., & Akinola, A. (2022a). Cybersecurity enhancement strategies in smart agricultural systems using IoT frameworks. *Journal of Digital Security and Agriculture*, 8(3), 45–56.
- Adewusi, A. O., Okechukwu, O., & Akinola, A. (2022b). Analysis of IoT vulnerabilities and countermeasures in agricultural networks. *International Journal of Information Security Research*, 11(2), 101–113.
- Afzal, S., Hussain, S., & Imran, A. (2021). A review of IoT vulnerabilities and cyber risks in smart agriculture systems. *Computers and Electronics in Agriculture*, 187, 106291.
- Al Asif, M., Hasan, R., & Islam, M. S. (2021). A STRIDE-based cyber threat model for IoT-enabled precision agriculture. *Journal of Cybersecurity and Digital Agriculture*, 9(4), 33–49.
- Arul Anitha, J., & Arockiam, L. (2022). An integrated security architecture for IoT-based precision agriculture. *International Journal of Advanced Computer Science and Applications*, 13(6), 58–66.
- Bakar, M., Jamaludin, N., & Omar, H. (n.d.). IoT security challenges in developing agricultural ecosystems. *Asian Journal of Smart Technologies*, 7(1), 21–30.
- Berguiga, M., Kherbouche, A., & Kaci, S. (2023). Enhancing IoT security through adaptive machine learning approaches. *IEEE Internet of Things Journal*, 10(5), 4213–4224.
- Bui, T. T., Pham, Q., & Nguyen, H. (2023). Hybrid intrusion detection systems for IoT environments using ensemble learning. *Sensors*, 23(2), 745–759.
- Campoverde-Molina, M., & Luján-Mora, S. (2024). Cybersecurity and resilience in Agriculture 4.0 systems: Challenges and frameworks. *Computers*, 13(1), 32–49.
- Chaudhary, R., & Patil, A. (2024). Cyber threats and mitigation approaches in digital agriculture: A survey. *Journal of Agricultural Informatics*, 15(1), 45–58.
- Dhirani, A., Khan, A., & Qureshi, F. (2021). Integrating rule-based logic with anomaly detection for IoT-based

- cyber defence. *Procedia Computer Science*, 200, 1124–1131.
- Islam, M. S., Rahman, M., & Al-Mamun, M. (2021). Applying STRIDE threat modelling to IoT-based smart home networks. *International Journal of Cybersecurity and Digital Systems*, 12(4), 29–44.
- Islam, M. S., Rahman, M., & Al-Mamun, M. (2022). Machine learning-based anomaly detection for IoT cyber resilience. *Sensors*, 22(18), 6712.
- Kumar, R., & Yadav, S. (2024). Lightweight security frameworks for IoT-based smart infrastructures. *Future Generation Computer Systems*, 153, 453–468.
- Lata, P., & Kumar, R. (n.d.). Isolation Forest-based anomaly detection in industrial IoT applications. *International Journal of Data and Network Security*, 9(1), 12–21.
- Liu, J., & Wang, Y. (2023). Comparative analysis of STRIDE, PASTA, and LINDDUN in IoT threat modelling. *Information Systems Security Journal*, 32(2), 87–99.
- Malik, H., Khan, S., & Farooq, U. (2021). IoT security analysis and mitigation in sensor-based agriculture. *IEEE Access*, 9, 110345–110358.
- Ouaissa, M., & Ouaissa, Y. (2025). Adaptive STRIDE implementation in IoT and cyber-physical systems. *International Journal of Advanced Computer Science*, 31(1), 77–90.
- Roy, P., Islam, M. S., & Chowdhury, M. (2022). Cyber risk analysis in smart solar IoT infrastructures using STRIDE. *Sustainable Computing: Informatics and Systems*, 35, 100751.
- Roy, P., Islam, M. S., & Chowdhury, M. (2023). Proactive cybersecurity approaches in precision agriculture networks. *Computers and Electronics in Agriculture*, 206, 107593.
- Subhash, P., Sharma, V., & Kaur, N. (2023). Extending STRIDE for general IoT risk assessment frameworks. *Journal of Information Security and Applications*, 75, 103415.
- Tang, J., & Chen, W. (2024). Adaptive threat modelling for live IoT systems using STRIDE and rule enforcement. *Journal of Network and Computer Applications*, 239, 104806.
- Üstebay, S., Kaya, E., & Tuncer, T. (2025). Enhancing zero-day attack detection in IoT networks via Isolation Forest and ensemble tree models. *Journal of Computer Networks and Applications*, 23(1), 61–77.
- Wang, L., & Luo, J. (2023). Real-time threat mitigation in IoT ecosystems through automated quarantine policies. *IEEE Access*, 11, 12245–12259.
- Yadav, R., & Prakash, D. (2024). Challenges of hybrid intrusion detection in agricultural IoT environments. *Computers*, 13(2), 114–129.
- Yin, Z., & Zhou, H. (2022). A multi-model hybrid IDS for IoT environments: Combining rule-based and anomaly detection. *Future Internet*, 14(12), 362.
- Zahoor, S., Khan, M. A., & Nazir, A. (2025). A hybrid intrusion detection framework combining Isolation Forest and One-Class SVM for IoT systems. *Journal of Information Security and Privacy*, 12(3), 203–219.
- Zhang, Y., Li, X., & Zhao, F. (2023). Machine learning-driven anomaly detection in IoT networks. *Computers and Electrical Engineering*, 109, 108764.