AI-Driven Cybersecurity in Smart Agriculture: Threats, Challenges, and Secure System Architectures

Chintan Hirpara[1],Khushi Kundariya[2],Mahipal Chothani[3],Deep Solanki[4],Jigar Gajjar[5]

LokJagruti Kendra University, Ahmedabad, GJ, India[1,2,3]
TechD Cybersecurity Limited, Ahmedabad, GJ, India[4,5]

chintanhirpara2707@gmail.com[1],kundariyakhushi0404@gmail.com[2], mahipalchothani5@gmail.com[3],
deepsolanki5799@gmail.com[4],cyberian.jg@gmail.com[5]

Abstract:Farming has changed dramatically over the past two decades. What once relied on a farmer's experience and physical labour now runs on sensors, AI algorithms, and cloud platforms — and that shift, while genuinely productive, has dragged agriculture into a cybersecurity threat landscape it was never designed to handle. IoT devices sitting in open fields, wireless networks spanning rural distances, and AI models quietly steering irrigation and harvest decisions each represent exploitable entry points for motivated attackers. Worse, most farmers lack cybersecurity training, devices run on default credentials, and no universal security standard exists for agricultural technology.

This paper addresses that gap through three contributions: a STRIDE-based threat analysis mapping adversarial risks to specific farm system components; a five-layer Security-by-Design architectural framework integrating AI-driven defences from physical surveillance through to supply-chain traceability; and algorithm-level specifications for the AI mechanisms within that framework. Cybersecurity in agriculture is no longer optional — it is a national food security requirement.

Keywords:Smart Agriculture, Cybersecurity, IoT, AI, STRIDE, Security-by-Design, Food Security, Machine Learning.

I. INTRODUCTION

Ask a farmer from the 1980s what tools they relied on, and the answer would centre on experience, physical intuition, and relatively simple mechanical equipment. Ask a farmer today, and the answer looks very different: soil moisture sensors, satellite imagery, AI-powered disease-detection dashboards, automated irrigation controllers, and cloud-based yield forecasting platforms [1], [7], [9]. This is not merely a change in tools — it is a change in the nature of farming itself.

Modern agriculture now operates on two parallel planes. The first is the familiar physical plane of land, crops, water, and machinery. The second is a digital plane of data streams, predictive models, networked controllers, and supply-chain records. What makes this arrangement both powerful and precarious is that the digital plane directly governs the physical one. A corrupted irrigation schedule can kill a crop. A ransomware attack on a farm management system can halt operations during the narrow window of harvest. A poisoned yield-prediction model can push a farmer to plant the wrong crop at the wrong density [2], [5], [12]. In each case, a digital threat produces a very physical consequence.

The problem is compounded by the realities of agricultural deployment. Many of the IoT devices used on farms are installed with factory-default credentials and receive firmware updates infrequently, if at all [6], [13]. The wireless networks linking these devices to farm management systems often traverse kilometres of open countryside with minimal physical security. Farmers and farm workers, while highly skilled in agronomy, rarely have formal cybersecurity training, and there is no universally adopted security standard for agricultural technology [4], [21]. Agriculture is meanwhile increasingly classified as critical national infrastructure [9], [22], meaning that a successful large-scale attack could destabilise food supply chains well beyond a single farm or region [2], [3].

http://doi.org/10.63766/spujstmr.26.000090

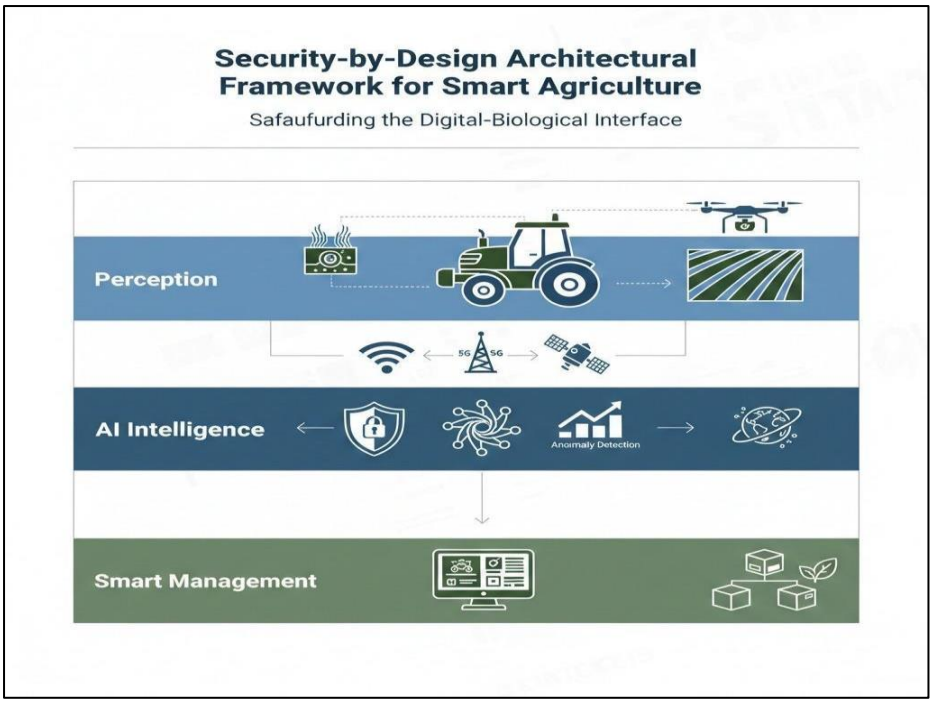

Fig.1. Security By Design Architectural Framework For Smart Agriculture

These technologies allow for early detection of crop disease, precision fertilizer application, automated irrigation control and forecasting of crop yields – all based on real-time data instead of relying on human intuition alone [11], [12]. Historically, experience was the primary deciding factor in agricultural decision making, however, with the fact that agriculture will be increasingly dependent upon ongoing collection of data and the use of digital intelligence in maximizing agricultural production and resource use [4], the need for cybersecurity in agriculture has greatly increased due to the higher levels of reliance on digital interconnectedness across agricultural production systems, along with the use of real-time data transfer on a daily basis, as a disruption of either data integrity or system availability can have a direct and negative impact on the decisions made regarding producing agriculture and farming, therefore making agriculture vulnerable to cyber threats [2], [5].

Smart agriculture, which is also known as precision agriculture, relies on things such as the Internet of Things and artificial intelligence to improve agriculture [1], [6]. It also relies on cloud computing and remote sensing and automation [4], [7]. All these help with farm management, ensuring that they are sustainable [9].

Sensors are placed in the fields where crops are grown and where animals are raised [7]. These sensors gather information all the time about the soil, how well crops are growing and what the weather is like and how healthy the animals are [10]. AI-based analytics examines this information to help determine how much food we can grow, find diseases in plants, use resources efficiently, and automate farming processes [6], [14]. These new technologies help farmers grow food, save money, cause less harm to the environment, and cope with changes in the weather [2], [3].

The truth is that there are some positive aspects of smart agriculture systems. However, people are using more and more of things. This means that there are dangers regarding cybersecurity [2], [5]. Smart agriculture systems employ many devices that are connected to the internet [3]. They communicate with each other through wireless communication and cloud technology [8]. All these can be hacked by hackers [13]. There is much information that is transmitted and stored through computers [12]. This information includes things such as how healthy the soil is how well the crops are doing what the weather is like, and information about the animals on the farm [3]. Smart agriculture systems are vulnerable because of this [5]. There are security mechanisms that are not good enough for these systems [13]. They can be vulnerable to threats such as people gaining unauthorized access to them, data breaches, and entering incorrect information [2]. Additionally, automated controls can be compromised [5]. The entire system can be brought to a complete halt [13]. This can be done because of security mechanisms. There are security mechanisms that are not good enough. These can cause much trouble [2], [5].

When these events occur, they may cause decisions to be made about farming people losing money things not working properly and farmers not trusting digital farming solutions because of inadequate security mechanisms

[2], [3]. Inadequate security mechanisms can have consequences [5].
Cybersecurity issues in farming are an issue [5]. The nature of farming makes these issues even larger [13]. Many devices that rely on the internet lack much power to process information and are also located in open areas or far from cities [6], [8].
Cybersecurity issues in agriculture are also exacerbated by the fact that farmers lack sufficient knowledge about cybersecurity [2]. Farmers tend to use the default settings of their devices [13]. They fail to update their software on a regular basis [5]. Cybersecurity issues in agriculture are further exacerbated by the fact that equipment is being used in conjunction with new digital technologies [8]. This makes it difficult to adopt security measures, for agriculture cybersecurity [5]. Agriculture is a part of our countrys critical infrastructure [3]. The issues with agriculture pose threats, to our food security, the economy, and the ability of our country to develop in a sustainable manner [2], [3]. Agriculture is a very important aspect. The threats posed are very serious. They may impact our food security, economic stability, and the development of our country over time which is why agriculture is a concern [8].

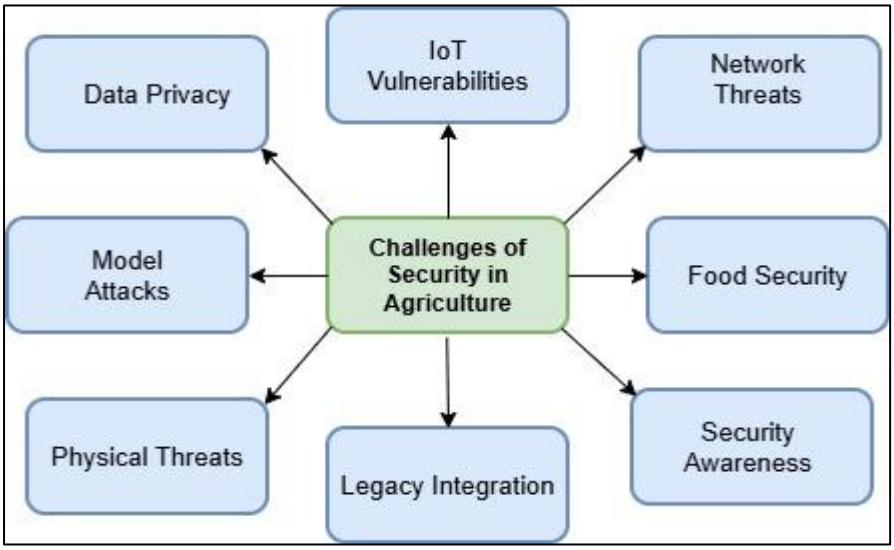

Fig.2 Challenges of Security Agriculture

Artificial intelligence is a very important thing when it comes to handling cybersecurity issues [6]. Artificial intelligence assists us in creating security systems that are capable of monitoring what is happening on our systems and devices all the time [5]. These systems are able to detect things that are not normal and prevent hackers from attacking us before they cause any harm [6].
Machine learning is a component of intelligence that assists us in detecting threats before they cause any harm [6]. It does this by identifying patterns that are not normal [13]. Intelligence and machine learning assist us in preventing bad things from happening to our systems and data [5]. Artificial intelligence is a tool that assists us in staying safe from cyber attacks [6]. AI-powered computer vision systems make our physical security systems even more secure by identifying people who are not supposed to be there or trying to tamper with agricultural equipment and systems that monitor our livestock [14].

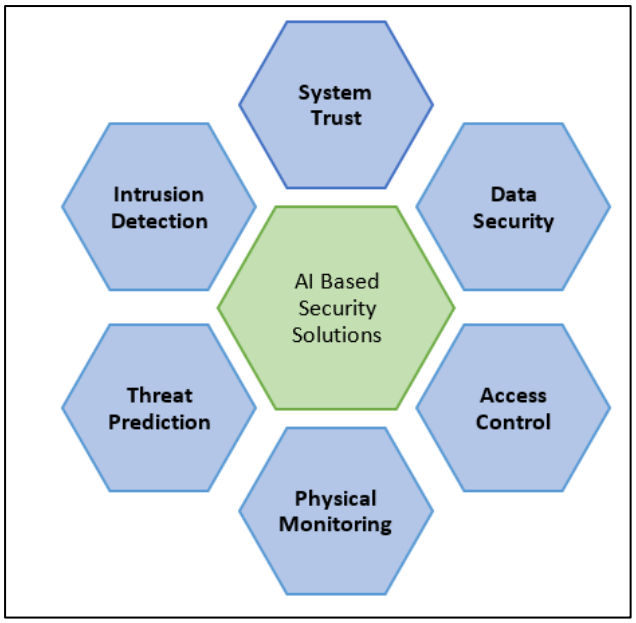

Fig.3 AI Based Security Solutions

The AI and blockchain technologies ensure that information is shared in a safe manner, and we are able to trace where everything comes from and that the information is right from the beginning of the agricultural supply chain to the end [12], [26], [27].

Smart and connected agriculture is very beneficial to agriculture because it assists farmers in growing food and doing so in a manner that is better for the environment [1], [9]. Smart and connected agriculture also assists farmers in working in an efficient manner [7]. Smart and connected agriculture will not be able to function in the right manner if there is not good cybersecurity [5]. This means that agriculture and artificial intelligence and cybersecurity must all work together [6]. When they do, we are able to develop trustworthy digital agricultural systems that can resist difficulties [8], [28]. Smart and connected agriculture is very important. Cybersecurity is also very important to smart and connected agriculture [2], [3].

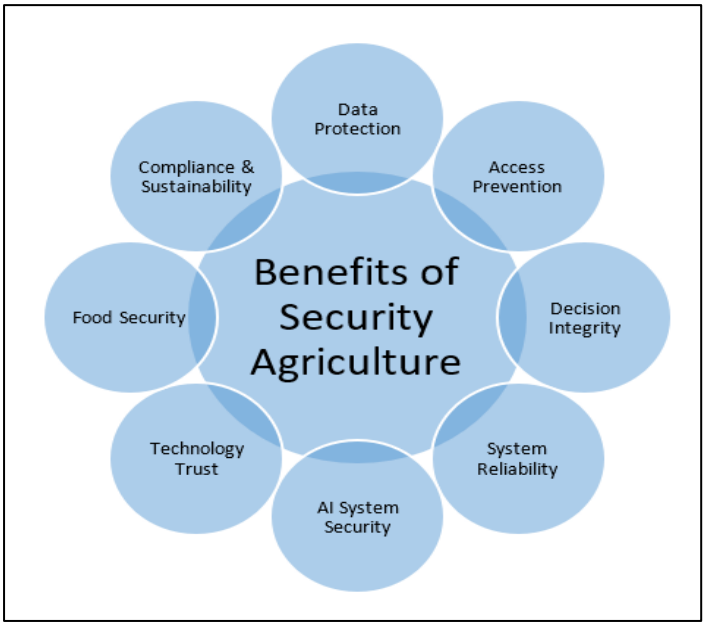

Fig.4 Why Security is Essential Agriculture

II. LITERATURE SURVEY AND RESEARCH GAP ANALYSIS

2.1 How Smart Agriculture Evolved

Farming's digital journey did not happen overnight. Early milestones in the late 1990s and early 2000s included computerised farm records, satellite-based remote sensing, and digital weather stations — tools that let farmers collect and examine data more systematically than ever before [9], [11]. The following decade brought wireless sensor networks and the first commercially viable IoT platforms, which made it possible to monitor field conditions continuously without walking the land [1], [7]. More recently, AI-powered analytics have layered intelligence on top of raw sensor data, enabling automated decision-making for tasks such as irrigation timing, pest-pressure forecasting, and livestock health monitoring [6], [8].

The result is a sector that, in its most advanced form, resembles a distributed computing network as much as it resembles a traditional farm. Precision irrigation reduces water consumption while holding or improving yields [7], [9]. Computer-vision models mounted on drones detect crop disease at a stage when intervention is still straightforward [8], [13]. Wearable sensors on livestock flag health anomalies before they become costly outbreaks [7], [25]. Blockchain-backed supply-chain records trace produce from soil to shelf with a transparency that was previously impossible [23], [26]. The productivity and sustainability arguments for these technologies are well established [19], [21]. Their security implications are considerably less studied.

2.2 What Existing Frameworks Get Right — and Where They Fall Short

A growing body of work has begun mapping the cybersecurity challenges of smart agriculture, and it is worth understanding what that work has and has not accomplished before introducing another framework.

Campoverde-Molina and Lujan-Mora [5] carried out a thorough systematic literature review covering IoT vulnerabilities, network exposure, and data security gaps in precision agriculture. Their contribution is valuable as a problem inventory, but they stopped short of proposing an integrateddefence architecture. Yazdinejad et al. [12] catalogued attack surfaces across a wide range of precision farming systems — sensors, communication links, AI models, and cloud platforms — with commendable technical specificity. Again, however, the analysis did not extend to a unified security framework with implementation guidance. Ferrag et al. [25] surveyed AI-based security mechanisms for smart farming and identified many of the same building blocks we adopt here, but they treated those mechanisms independently rather than as layers in a coordinated architecture. Perhaps closest to the present work is the STRIDE-based threat modelling exercise of Al Asif et al. [28], which provided a principled structure for enumerating threats in IoT-enabled precision agriculture. Their work focuses on threat identification; ours extends that foundation to a mitigation architecture with specified AI components.

Three gaps run consistently through the existing literature. First, cybersecurity mechanisms are almost always discussed in isolation. No prior work integrates physical security, device authentication, network defence, model integrity assurance, and supply-chain protection into a single, layered architecture. Second, proposed AI defences are routinely described at a conceptual level — 'use anomaly detection,' 'apply machine learning' — without specifying algorithms, features, or measurable targets. Third, the connection between agricultural cybersecurity and national food security strategy has not been formally framed within a Security-by-Design context that could inform policy as well as engineering.

2.3 Security Challenges in Smart Agriculture Systems

2.3.1 Data Collection and Integrity

Today's farms generate an enormous volume of sensitive data: granular soil chemistry readings, hourly crop growth measurements, weather records, and detailed livestock health logs [7], [10]. That data feeds AI models which, in turn, drive decisions with real financial and agronomic consequences. An adversary who can alter even a modest fraction of incoming sensor readings — pushing soil moisture values below actual levels to trigger unnecessary irrigation, for instance — can cause direct operational harm while remaining undetected for days or weeks [2], [5], [9]. The challenge is that the sheer volume of data collected makes manual verification impractical, which is exactly why automated integrity monitoring is essential.

2.3.2 IoT Device Vulnerabilities

A mid-sized precision farm might deploy hundreds of IoT devices: soil sensors, climate monitors, livestock trackers, irrigation controllers, aerial drones, and edge gateways [1], [6], [12]. Many of these devices are computationally limited,

which constrains the cryptographic protocols they can run. Many are installed outdoors, far from physical oversight, making them accessible to anyone who walks into a field. And many stay in service for years without firmware updates, accumulating unpatched vulnerabilities over time [6], [13]. When a single compromised device is used as a beachhead to move laterally across a farm network, the consequences can extend well beyond that one sensor — from ransomware deployment on the central management system to DDoS attacks launched from the farm's own equipment [6], [12], [16].

2.3.3 Insecure Wireless Communications

Rural wireless networks — the arteries that carry data between field devices and farm management systems — operate across open terrain where signal interception is straightforward [7], [16], [17]. Without proper encryption and authentication at the network layer, an attacker positioned within radio range can eavesdrop on data transmissions, spoof sensor identities to inject false readings, or conduct Man-in-the-Middle attacks to intercept and alter commands before they reach automated field equipment [5], [12]. These threats are not theoretical; the relative openness of rural environments makes them considerably easier to execute than comparable attacks in urban or industrial settings.

2.3.4 Adversarial Attacks on AI Models

The AI models that power smart agriculture — forecasting yields, detecting plant disease, scheduling irrigation — are themselves attack targets, and this is perhaps the least appreciated risk in the sector. Data poisoning introduces corrupted or strategically crafted records during the training phase, causing a model to learn systematically wrong associations [4], [6], [12]. Evasion attacks craft inputs that reliably cause a deployed model to misclassify at inference time. Model inversion attacks attempt to extract sensitive information embedded in a trained model's parameters [18]. What makes these threats particularly insidious is that they can degrade model performance gradually and silently, producing decisions that seem plausible until the accumulated damage becomes visible in crop outcomes weeks or months later [3], [9].

2.3.5 Physical Security of Field Equipment

It is easy to focus on cyber threats and overlook the physical dimension, but the two are tightly coupled in agricultural settings. A sensor that is physically tampered with can be made to transmit false data while appearing operationally normal. A gateway whose housing is opened and whose cryptographic keys are extracted becomes a permanent backdoor into the farm network [2], [5], [13]. Devices stolen from the field carry configuration data and credentials that an attacker can analyse offline [12], [16]. Physical and cyber security must therefore be addressed together rather than sequentially.

2.3.6 Integrating Legacy Equipment

Many farms have invested heavily in equipment that was designed before network connectivity was standard — tractors with proprietary control systems, irrigation infrastructure with analogue controllers, storage facilities with minimal instrumentation [12], [19]. Connecting this legacy equipment to modern IoT and AI platforms is often necessary for operational continuity, but it creates security gaps that neither the old equipment nor the new platforms were designed to handle. Legacy systems frequently lack support for contemporary encryption standards, do not accept software patches, and expose network interfaces that were never intended to face an adversarial environment [3], [6], [20].

2.3.7 Human Factors and Awareness Gaps

Technical vulnerabilities do not exist in a vacuum; they are exploited through human behaviour. Farmers and agricultural workers who use default device passwords, skip software updates, or share network access credentials inadvertently create pathways that even moderately skilled attackers can follow [4], [10], [21]. The challenge here is not carelessness — it is that cybersecurity literacy has simply not been part of agricultural training, and the available guidance is rarely tailored to the specific context of farm operations [6], [12]. Awareness programmes and practical, farm-specific security checklists are a necessary complement to the technical measures discussed elsewhere in this paper.

2.3.8 Food Security at the National Scale

The consequences of agricultural cyber-attacks do not stop at the farm gate. Agriculture is formally classified as critical national infrastructure in many countries [9], [10], [22], which means that coordinated attacks on farming systems can have cascading effects on food supply chains, rural employment, commodity prices, and ultimately consumer access to food [1], [3], [23]. The potential for this kind of large-scale, cross-sector impact is what lifts agricultural cybersecurity from a niche technical concern to a matter of national strategy. Any serious policy framework for critical infrastructure

protection needs to include smart agriculture explicitly, with associated minimum security standards and incident reporting obligations.

TABLE I
USE CASES OF AGRITECH AND ITS BENEFITS

Agritech Use Case	**Technology Involved**	**Benefits**
Precision Irrigation [1], [7], [9]	IoT sensors, AI analytics	Optimizes water usage, reduces wastage, and improves crop yield
Crop Disease Detection [8], [13]	AI, computer vision, drones	Early detection of plant diseases and reduced crop loss
Smart Soil Monitoring [4], [9]	IoT sensors, cloud platforms	Real-time soil analysis and efficient nutrient management
Livestock Monitoring [7], [25]	Wearable sensors, IoT, AI	Improves animal health, productivity, and disease prevention
Automated Farming Machinery [20], [24]	Robotics, automation	Reduces labor dependency and increases operational efficiency
Smart Supply Chain Management [23], [26]	Blockchain, cloud computing	Enhances traceability, transparency, and reduces post-harvest losses
Weather Forecasting Systems [19], [21]	AI, big data analytics	Improves climate-resilient farming and risk management
Smart Greenhouse Management [4], [8]	IoT, automation, AI	Maintains optimal growth conditions and increases crop quality
Yield Prediction Systems [19], [21]	Machine learning, data analytics	Accurate yield estimation and better farm planning
Farm Security Monitoring [6], [27]	AI, computer vision, IoT	Prevents theft, intrusion, and equipment tampering

TABLE II
.SMART AGRICULTURE SECURITY ARCHITECTURE USING AI TECHNOLOGIES

Security Area	**AI Technology Used**	**Problem Addressed**	**Security Benefit**
Intrusion Detection [6], [22]	Machine Learning, Deep Learning	Cyberattacks on IoT networks and farm systems	Early detection of attacks and reduced system downtime
Secure Data Access [5], [23]	AI-based access control	Unauthorized access to sensitive farm data	Improved data privacy and confidentiality
Device Authentication [12], [25]	Behavioral AI models	Fake or compromised IoT devices	Ensures only trusted devices operate in the network
Threat Prediction [6], [27]	Predictive analytics, AI models	Unexpected cyberand operational risks	Proactive security and risk mitigation
Physical Asset Protection [12], [27]	Computer vision, AI drones	Theft, vandalism, and tampering of devices	Real-time monitoring and rapid

			response
Data Integrity Monitoring [3], [22]	AI anomaly detection	False data injection and data manipulation	Reliable decision-making and accurate AI outputs

II. ANALYSIS

Structured threat modelling is a discipline that forces security analysis to be systematic and reproducible rather than intuitive and ad hoc. The STRIDE methodology, originally developed at Microsoft and subsequently applied across a wide range of critical systems [28], organises threats into six categories: Spoofing (impersonating a legitimate entity), Tampering (modifying data or code), Repudiation (denying an action without the possibility of proof), Information Disclosure (exposing data to unauthorised parties), Denial of Service (making a resource unavailable), and Elevation of Privilege (gaining access beyond what is authorised).

We applied STRIDE to a representative smart agriculture architecture comprising field-deployed IoT sensors, edge gateways, wireless communication infrastructure, cloud-hosted farm management software, AI analytics modules, and supply-chain record systems. Table III presents the results of this analysis, mapping each threat category to the specific agricultural components it affects, realistic adversarial scenarios, and the countermeasures incorporated into the Security-by-Design framework described in Section IV.

A pattern that emerges clearly from this analysis is that no single countermeasure can address the full range of threats. Encrypting network communications helps against Tampering but does nothing for a Spoofing attack that uses valid credentials. Blockchain audit trails address Repudiation but do not protect against Denial of Service. This multi-dimensional threat landscape is precisely why a layered architecture, rather than a collection of point solutions, is the appropriate design response — which is what Section IV proposes.

TABLE III

INTEGRATED ANALYSIS OF AI-ENABLED SMART AGRICULTURE AND SECURITY

Aspect	**Traditional Agriculture**	**Smart Agriculture (AI + IoT)**	**Key Security Risk**	**AI-Driven Security Impact**
Decision Making [1], [6]	Experience-based	Data-driven, real-time	Data manipulation	Trustworthy analytics
Data Generation [5], [22]	Minimal	Massive sensor data	Data leakage	Secure data validation
Connectivity [12], [25]	Stand-alone systems	Highly interconnected	Network attacks	Intelligent intrusion detection
Automation Level [6], [27]	Manual operations	Autonomous systems	Control hijacking	Behavioral monitoring
Resource Usage [19], [21]	Inefficient	Precision optimized	False input injection	Accurate AI filtering
Infrastructure [5], [23]	Isolated	Cloud &IoT dependent	Cloud breaches	Encrypted access control
Physical Security [12], [27]	Human-guard	Sensor-dependent	Device tampering	AI vision surveillance
Scalability [26], [27]	Limited	Highly scalable	Attack surface growth	Predictive risk control
Farmer	Human	AI	Model	Model integrity

Dependence [6], [22]	judgement	recommendations	poisoning	checks
National Impact [9], [25]	Localized	Critical infrastructure	Food supply disruption	Resilient system design

IV. A SECURITY-BY-DESIGN ARCHITECTURAL FRAMEWORK FOR SMART AGRICULTURE

4.1 Design Principles

The Security-by-Design concept holds that security is most effective when it is built into a system from the ground up rather than bolted on after deployment [5], [12], [25]. Four principles guided the design of the framework proposed here, each derived directly from the threat landscape and the research gaps identified in the preceding sections.

Proactive rather than reactive defence: Given how quietly threats like data poisoning and behavioural anomalies can accumulate, security mechanisms need to detect and respond to threats before operational damage materialises — not after a crop has failed or a data breach has been reported.

Layered, interlocking protection: Because no single mechanism covers the full STRIDE landscape, the framework organisesdefences into five distinct layers, each addressing a specific class of threat while sharing intelligence with adjacent layers.

Autonomous operation: Most agricultural IoT infrastructure operates in remote locations with limited human oversight. Security systems must therefore be capable of running, adapting, and partially self-repairing without requiring continuous manual intervention.

Backward compatibility with legacy systems: The framework must accommodate farms that mix modern IoT-native equipment with older machinery that predates network connectivity, using standardised interfaces to bridge the security gap between the two generations.

4.2 The Five-Layer Architecture

The proposed SbD framework is structured as five functional security layers. Together they form a closed-loop architecture in which threat intelligence gathered at each layer informs the adaptive responses of the others. The layers and their properties are summarised in Table IV.

4.3 AI Security Mechanism Specifications

One of the most persistent weaknesses in the agricultural cybersecurity literature is the gap between naming an AI-based defence and actually specifying how it works. Saying that a system uses 'anomaly detection' or 'machine learning authentication' is not enough to enable replication, benchmarking, or procurement decisions. This section closes that gap for three core AI mechanisms within the SbD framework.

4.3.1 Network Anomaly Detection (Layer 3)

The network layer intrusion detection system works by learning what normal traffic looks like across every class of device on the farm network, then flagging deviations from that baseline. Three complementary algorithm families are appropriate here, depending on available labelled data and deployment constraints [6], [12], [24].

Isolation Forest is well suited to unsupervised deployment scenarios where labelled attack examples are unavailable, as is common in agricultural contexts. It isolates anomalies by randomly partitioning the feature space: records that are easy to isolate (requiring few partitions) are flagged as outliers. Random Forest classifiers offer higher accuracy when a labelled dataset of attack and normal traffic is available, producing probabilistic attack classifications that can be tuned to favour low false-positive rates. LSTM networks are particularly valuable for detecting temporal anomalies in the time-series data

generated by agricultural sensors, capturing sequential patterns — such as gradual data drift from a compromised sensor — that point-in-time classifiers would miss.

The feature set covers: packet inter-arrival time, payload length distribution per device class, protocol distribution per time window, connection duration, bytes transferred per session, and the number of unique destination addresses observed per hour. Normal behavioural baselines are established per device class (sensors, gateways, drones) during a supervised initialisation phase lasting a minimum of 30 days. Deviations exceeding a configurable threshold — we recommend three standard deviations from the learned baseline as a starting point — trigger graduated responses ranging from operator alert through to automatic network isolation of the suspect device. Target performance benchmarks, derived from comparable IoT deployment evaluations in the literature [6], [25], are: Detection Rate above 95%, False Positive Rate below 2%, and mean time to detection under 60 seconds.

4.3.2 Behavioural IoT Device Authentication (Layer 2)

Static credentials — passwords, certificates — are a necessary but insufficient foundation for IoT authentication in agricultural settings. Credentials can be stolen from a device physically, replayed from captured traffic, or remain valid long after a device has been physically compromised [4], [12]. Behavioural authentication addresses this by treating each device's operational patterns as a continuous identity signal.

The model is trained on the legitimate operational behaviour of each device class using features that include: message transmission interval (with device-specific variance bounds), payload entropy over rolling windows, communication partner set (which other devices or servers does this device talk to, and how often), time-of-day activity distribution, and power draw patterns where hardware monitoring is available. A One-Class Support Vector Machine trained exclusively on legitimate device behaviour is computationally tractable on edge hardware and produces a real-time trust score for each device. For deployments where edge computational resources allow, an Autoencoder neural network offers higher sensitivity to subtle behavioural drift at the cost of greater processing demand.

Devices whose behavioural profile exceeds the learned trust boundary are quarantined and flagged for manual review. Crucially, this mechanism catches a class of attack that credential-based systems miss entirely: the device that has valid credentials but is being remotely controlled by an attacker after firmware compromise. The change in communication behaviour — different destination addresses, altered message cadence, unusual payload sizes — triggers quarantine even though the device's certificate remains valid [5], [18].

4.3.3 Predictive Threat Assessment (Cross-Layer)

The five layers of the SbD framework generate a continuous stream of security signals: physical intrusion alerts from L1, device trust scores from L2, traffic anomaly flags from L3, data integrity verdicts from L4, and supply-chain tamper notifications from L5. A cross-layer predictive threat assessment module aggregates these signals to produce a system-wide risk picture and generate prioritised mitigation recommendations [6], [27].

The core model is a gradient-boosted decision tree ensemble — XGBoost is the recommended implementation given its performance on tabular security event data and its interpretability relative to deep learning alternatives. The model is trained on historical agricultural cyber-incident records, enriched with contextual features such as crop growth stage (certain attack types are more likely during high-value harvest windows), seasonal patterns, recent software vulnerability disclosures relevant to the farm's device inventory, and weather conditions (extreme weather events have historically correlated with increased physical intrusion attempts in agricultural settings).

Outputs are designed to be actionable by farm operators without cybersecurity expertise: a probabilistic risk score for the next 24-hour operational window expressed as low, medium, or high; a ranked list of the three highest-priority vulnerabilities currently active in the system; and specific recommended countermeasure actions phrased in operational rather than technical terms. The module interfaces directly with farm management dashboards, surfacing this intelligence alongside agronomic data so that security context is available at the same decision-making touchpoint farmers already use.

III. CONCLUSION

Smart agriculture has arrived. The technologies that make precision farming possible — IoT sensor networks, AI analytics, automated control systems, cloud platforms, blockchain supply chains — are already deployed on farms around

the world and their adoption is accelerating. The productivity and sustainability gains they enable are real. So, unfortunately, are the security risks they introduce.

This paper has tried to do three things that the existing literature has not done together in one place. The first was to apply structured threat modelling — specifically STRIDE — to a representative smart agriculture system, producing a map of adversarial threats that is systematic and reproducible rather than intuitive and anecdotal. The second was to propose a Security-by-Design framework that addresses those threats through five interlocking defensive layers, from physical asset protection in the field through to blockchain-secured supply-chain traceability. The third was to move beyond the conceptual level that characterises most AI security proposals in this domain, specifying the machine learning algorithms, feature engineering choices, and measurable performance benchmarks for the AI mechanisms inside the framework.

Running through all three contributions is a single argument: agricultural cybersecurity is not a peripheral IT problem. It is a foundational requirement for the food systems that nations depend on. When automated irrigation fails because of a cyber-attack, crops die. When AI yield models are poisoned, farmers make decisions on corrupted intelligence. When supply-chain records are tampered with, food safety and trade systems break down. The digital plane of modern agriculture is not separate from the physical plane — it governs it. Securing one means securing the other.

Several important tasks remain for future research. The AI mechanisms specified in Section 4.3 need empirical validation on real-world agricultural IoT datasets; without that, the performance benchmarks proposed here remain targets rather than demonstrated capabilities. The behavioural authentication model needs lightweight implementations that can run on the constrained hardware typical of field-deployed sensors without sacrificing detection sensitivity. Federated learning approaches deserve investigation as a way to train security models across distributed farm networks without requiring sensitive operational data to leave individual farms. And longitudinal field studies — tracking how the SbD framework performs in actual farm environments over full growing seasons, and what effect farmer training programmes have on the human-factor vulnerabilities identified in Section 2.3.7 — are needed to ground the framework's design in operational reality. These are not small tasks, but they are the right next steps

REFERENCES

[1] A. Akbar et al., “Smart farming technologies: Transforming agriculture through IoT and AI,” *Spectrum of Engineering Sciences, vol. 3, no. 5, pp. 929–936, 2025.*

[2] B. Singh and S. S. Cheema, “Cybersecurity threats and mitigation strategies in Agriculture 4.0 and 5.0: Challenges and solutions in the digital transformation of agriculture,” *Journal of Punjab Academy of Sciences, vol. 24, pp. 15–32, 2024.*

[3] P. Kaviya, M. Natarajan, and P. Ragulprasath, “Cybersecurity threats in digital agriculture: A systematic review on emerging risks and protective strategies for farmers,” *Asian Journal of Agricultural Extension, Economics & Sociology, vol. 43, no. 12, pp. 109–117, 2025.*

[4] M. U. Ali, “Smart agriculture: Integration of IoT, AI, and big data in farm management,” *Journal of Scientific Research and Reports, vol. 31, no. 12, pp. 114–122, 2025.*

[5] M. Campoverde-Molina and S. Luján-Mora, “Cybersecurity in smart agriculture: A systematic literature review,” *Computers & Security, vol. 150, Art. no. 104284, 2025.*

[6] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, “A survey on artificial intelligence in cybersecurity for smart agriculture,” *Mesopotamian Journal of Computer Science, vol. 2024, 2024.*

[7] A. Cisse et al., “A smart farming management system based on IoT technologies for sustainable agriculture,” *Advances in Science, Technology and Engineering Systems Journal, vol. 9, no. 1, pp. 1–8, 2024.*

[8] T. Miller, G. Mikiciuk, I. Durlik, M. Mikiciuk, A. Łobodzińska, and M. Śnieg, “The IoT and AI in agriculture: The time is now—A systematic review of smart sensing technologies,” *Sensors, vol. 25, no. 12, Art. no. 3583, 2025.*

[9] V. R. Pathmudi, N. Khatri, S. Kumar, A. S. H. Abdul-Qawy, and A. K. Vyas, “A systematic review of IoT technologies and their constituents for smart and sustainable agriculture applications,” *Scientific African, vol. 19, Art. no. e01577, 2023.*

[10] M. Roopaei et al., “Cloud of Things in smart agriculture: Intelligent irrigation monitoring,” *IEEE Cloud Computing, 2017.*

[11] S. Bimonte et al., “Data engineering for sustainable agriculture: Developments, challenges, and case studies of a novel IoRT architecture,” *Journal of Big Data, vol. 12, no. 1, Art. no. 195, 2025.*

[12] A. Yazdinejad et al., "Security of smart farming and precision agriculture: Attacks, threats, and countermeasures," *Applied Sciences, vol. 11, no. 16, Art. no. 7518, 2021*.

[13] A. S. Ibrahim et al., "AI-IoT based smart agriculture pivot for plant disease detection and treatment," *Scientific Reports, vol. 15, no. 1, Art. no. 16576, 2025.*

[14] A. K. Panda, S. D. Thakur, Kavita, R. Rameswar, R. S. Rana, and J. Singh, "Role of cow dung, cow urine, and other cow products in natural and organic farming," *International Journal of Agriculture Sciences, vol. 10, 2018.*

[15] S. Banerjee, A. Kanaujia, and S. Sharma, "Importance of indigenous cow dung and its microbiota," *International Journal of Current Microbiology and Applied Sciences, vol. 9, 2020.*

[16] A. K. Behera and C. P. Chandrashekara, "Effect of natural farming, organic farming, and recommended package of practices on yield and economics of irrigated wheat (Triticumaestivum)," *Indian Journal of Agronomy, vol. 66, 2021.*

[17] S. Tahura et al., "Combined application of biochar compost and cow urine enhances organic rice production," *Scientific Reports, vol. 12, 2022.*

[18] P. V. Patel et al., "A case study of cow-based organic farming system adopted by the farmer of Vadal, Junagadh, Gujarat," *International Journal of Chemical Studies, vol. 7, 2019.*

[19] L. Wolfert, S. Ge, C. Verdouw, and M. J. Bogaardt, "Big data in smart farming – A review," *Agricultural Systems, vol. 153, pp. 69–80, 2017.*

[20] F. Tao, Q. Zhang, J. Liu, and D. Lai, "Digital twin driven smart manufacturing," *Journal of Manufacturing Systems, vol. 58, pp. 103–118, 2021.*

[21] M. Kamilaris, A. Kartakoullis, and F. X. Prenafeta-Boldú, "A review on the practice of big data analysis in agriculture," *Computers and Electronics in Agriculture, vol. 143, pp. 23–37, 2017.*

[22] S. Misra, A. Mukherjee, and M. Obaidat, "Security challenges and approaches in Internet of Things-based smart agriculture," *IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4934–4946, 2020.*

[23] Y. Zhang, L. Wang, and H. Sun, "Blockchain-based secure data sharing for agricultural supply chains," *Future Generation Computer Systems, vol. 109, pp. 593–602, 2020.*

[24] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Computers and Electronics in Agriculture, vol. 157, pp. 218–231, 2019.*

[25] N. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Security for smart agriculture: A survey," *IEEE Access, vol. 8, pp. 160, 000–160, 018, 2020.*

[26] S. Halder, M. R. Islam, Q. Mamun, A. Mahboubi, P. Walsh, and M. Z. Islam, "A comprehensive survey on AI-enabled secure social industrial Internet of Things in the agri-food supply chain," *Smart Agricultural Technology, vol. 11, Art. no. 100902, 2025, doi: 10.1016/j.atech.2025.100902.*

[27] A. R. Mahlous, "Security analysis in smart agriculture: Insights from a cyber-physical system application," *Computers, Materials & Continua, vol. 79, no. 3, pp. 4781–4803, 2024, doi: 10.32604/cmc.2024.050821.*

[28] M. R. Al Asif, K. F. Hasan, M. Z. Islam, and R. Khondoker, "STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems," *arXiv, Jan. 2022.*