Can Cross-Layer Intrusion Detection Secure Agriculture 4.0 Systems?

Christiana Ioannou
School of Sciences
UCLan Cyprus
Larnaca, Cyprus
CEAIoannou@uclan.ac.uk
https://orcid.org/0000-0001-7332-4530

Chrysostomos Chrysostomou
Department of Electrical Engineering, Computer Engineering and Informatics
Frederick University
Nicosia, Cyprus
ch.chrysostomou@frederick.ac.cy
https://orcid.org/0000-0002-9287-990X

***Abstract*—Agriculture 4.0 leverages the Internet of Things (IoT), advanced communication technologies, and artificial intelligence (AI) to improve agriculture efficiency, optimize resource utilization, and promote sustainable crop production. IoT devices continuously monitor environmental conditions and transmit data to enable real-time decision-making in agricultural operations. However, the increased connectivity also expands the attack surface, exposing critical agricultural infrastructures to diverse cyber threats. Current intrusion detection systems (IDSs) primarily focus on detecting external attacks at isolated layers, often neglecting challenges related to data integrity, such as silent data corruption, sensor inconsistencies, and cross-layer anomalies. In this paper, we review existing IDS approaches and emphasize the need for a comprehensive system design methodology that addresses these challenges across all layers of Agriculture 4.0 systems. We propose DIVA-IDS, a cross-layer framework that integrates data integrity validation and anomaly detection to provide robust security for agricultural IoT environments. The framework aims to ensure reliable and secure data transmission, supporting the coexistence of various agricultural applications with differing security priorities.**

***Index Terms*—Agriculture 4.0, Cross-layer Intrusion Detection, Anomaly Detection, Internet of Things, Data Integrity.**

I. Introduction

The Internet of Things (IoT) enables the real-time communication of data from the environment to end users, supporting informed decision making that can ultimately save both time and money. One of the primary sectors that can benefit significantly from IoT is Agriculture 4.0, where real-time data collection replaces manual, time-consuming, and costly processes, while simultaneously increasing productivity. Agriculture 4.0 encompasses a wide range of applications, including precision farming, smart irrigation, automated harvesting, and predictive maintenance of agricultural machinery. These applications share the common goal of improving operational efficiency, enabling fast and reliable decision-making, and ultimately enhancing crop yields and sustainability [1]. The performance of these applications depends on the strategic deployment of sensors to collect the accurate and critical information necessary for real-time decisions.

Although the implementation of IoT-based systems in Agriculture 4.0 involves a considerable investment in both hardware and software, the anticipated gains in productivity and efficiency are expected to outweigh the initial costs. Depending on the specific application, sensors can include drones, pH meters, rainfall sensors, and other specialized devices [1]. These sensors are often used in harsh outdoor environments, and their performance, including lifespan and accuracy, is affected by environmental conditions [2].

The data collected from these sensors are transmitted through wireless sensor networks (WSNs), typically flowing from sensor nodes to a base station, then to a gateway or edge device, and finally to the cloud [2]–[4]. There are three main layers of the pipeline: the perception layer, which involves sensor readings; the network layer, which handles data transmission; and the application layer, where data is used to monitor and manage the environment [5]. Each layer introduces risks and threats that can change the flow of data.

As with any interconnected system, including legacy networks and IoT-based infrastructures, security remains a critical concern. The heterogeneity of IoT devices and the use of various communication protocols create multiple potential entry points, which can be exploited by external actors to disrupt operations, corrupt data, or manipulate system behavior. As highlighted in [5], the interconnected nature of these layers also introduces the possibility of cross-layer attacks, where an intrusion into one layer can compromise the security and integrity of others.

Intrusion Detection Systems (IDS) have long been proposed to use Artificial Intelligence (AI) tools to detect unauthorized intrusions [6]. In Agriculture 4.0, multiple IDS have been proposed that aim to detect attacks at different layers or during transmission of the data between the layers [5]. AI mechanisms are used to detect anomalies in the flow of data, which will indicate either an attack or even a fault or malfunction in the line of process. However, a critical challenge remains: many existing IDS solutions focus on specific layers or threat types, failing to address the systemic risks posed by cross-layer attacks and the potential for data corruption due to both malicious and non-malicious causes [2].

This paper argues that reliable decision-making in Agriculture 4.0 requires a new class of IDS frameworks

that integrate cross-layer data integrity validation with collaborative anomaly detection, ensuring that agricultural systems are secure, resilient, and trustworthy at every level of operation. The proposed framework, DIVA-IDS (Data Integrity Validation and Anomaly Detection Intrusion Detection System), addresses not only traditional intrusion attempts but also the equally significant issue of data anomalies arising from sensor faults, environmental factors, or hardware degradation. By validating data integrity across multiple layers and leveraging collaborative anomaly detection techniques, DIVA-IDS provides a more comprehensive and robust defense against the diverse threats and challenges facing Agriculture 4.0 systems.

The rest of the paper is structured as follows: Section II discusses the possible cyber attacks in the Agriculture 4.0 layers. Section III presents existing IDS in Agriculture 4.0, their deployment location and techniques used to detect anomalies. Section IV-C discusses the need for cross-layer IDS and presents DIVA a generic cross-layer framework that can be adapted based on the Agriculture 4.0 architecture to be deployed.

II. Cyberattacks in Agriculture 4.0

Agriculture 4.0 relies on reliable, timely data to make fast and effective decisions that can yield improved productivity. To achieve this, the data collected and transmitted must be protected, starting from the physical layer up to the application layer. There are three layers of security to consider: the preventive layer, the detection layer, and the reactive layer [7]. The preventive layer implements methods to ensure data integrity and confidentiality. Preventive methods include physical security, encryption, and firewalls. The selection of the preventive measure depends on the location in which the tool will be applied. In the physical layer, encryption can be used to secure data, whereas firewalls can be deployed at the edge. However, these preventive measures are not foolproof and can be bypassed or compromised, especially in a complex, interconnected environment like Agriculture 4.0.

The detection layer refers to the methods used to identify the presence of an attack. At this stage, the attacker has successfully bypassed the preventive layer and launched an attack. Detecting the attack on time is critical, which requires continuous monitoring of the area of interest to detect known or unknown threats at an early stage, thus avoiding potentially irreversible damage. Once the attack is identified, incident response procedures should be activated in order to restore the system and prevent future occurrences. Furthermore, in Agriculture 4.0, the detection layer must also account for anomalies that are not necessarily the result of malicious activity but may result from sensor malfunction, environmental factors, or data transmission errors [2]. When an attack or anomaly is detected, the reactive layer engages automated or manual recovery processes to restore the system to its defined operational baseline.

The current work is focused on the detection layer, in which the intruder has managed to penetrate the preventive defenses and gained access to the network, potentially launching different types of attacks. The detection layer requires constant monitoring of the target environment and an understanding of potential attack patterns. This enables the evaluation of the activity of the smart device and / or the network, which can then be analyzed using pattern-based detection, i.e., matching behavior against known attack signatures, or anomaly-based detection, which identifies deviations from established norms and may capture previously unknown or emerging threats. A critical aspect of the detection layer in Agriculture 4.0 is the ability to differentiate between malicious intrusions and data anomalies caused by non-malicious factors, requiring a more nuanced and context-aware approach than traditional security models.

Understanding the types of attacks associated with each architectural layer is essential for designing effective intrusion detection mechanisms. Each layer introduces different vulnerabilities and threats [8]. By recognizing the specific threat landscape at each layer, it becomes possible to select appropriate detection strategies, improve accuracy, and reduce the risk of false alarms or undetected attacks. However, in Agriculture 4.0, the interactions between layers create opportunities for cross-layer attacks, where an attacker may exploit vulnerabilities in multiple layers simultaneously to achieve a more significant impact or evade detection. This underscores the need for security measures that span across layers, providing a holistic view of the system's security posture.

The remainder of this section presents the different types of attacks encountered at each Agriculture 4.0 layer that an IDS is capable of detecting, reinforcing the need for a cross-layer, context-aware, and adaptive detection approach. This includes not only traditional cyberattacks but also data anomalies resulting from sensor failures or environmental factors. Such an approach is crucial in ensuring data reliability, which is paramount for the success of Agriculture 4.0.

A. Perception Layer

The perception layer includes the hardware and smart devices installed in the field to monitor the environment by gathering data. The choice of hardware and the type of data depend on the needs of the Smart Application and its aim, as well as the location of the field.

The primary aim of an attacker at the perception or physical layer is to manipulate the data. This can be achieved by altering sensor readings, injecting false data, or even tampering with the hardware. Data disruption can also occur through physical corruption of the hardware itself. The limited lifetime of hardware may cause incorrect readings, and harsh environments can diminish the quality of the data. In smart devices, such as drones, anomalies can inevitably occur. Addressing these vulnerabilities requires a detection approach that considers both malicious intrusions and non-malicious data anomalies. Attacks and data corruption scenarios in this layer include the following:

- **Sensor spoofing:** Attackers can inject false environmental data to mislead decision-making processes.
- **Side-channel attacks:** Attackers may extract sensitive information from the physical hardware to manipulate the system.
- **Physical tampering or unauthorized access:** Physical access to sensors allows attackers to directly manipulate or disable them.
- **Hardware Trojan attacks:** These attacks involve inserting malicious hardware components into the system.
- **Signal jamming/RF interference:** Disrupting wireless communication signals can prevent data transmission.
- **Silent Data Corruption (SDC):** Data errors caused by environmental stress, wear, or firmware attacks can go undetected [2].
- **Calibration attacks:** Attackers can gradually alter data output to degrade trust or performance over time.

B. Network Layer

Transmitting data can also cause anomalies that interfere with proper data transmission. In addition, vulnerabilities in network protocols and communication channels can be exploited to disrupt data flow or inject malicious content. Potential threats in the network layer are:

- **Man-in-the-Middle (MitM) attacks:** Attackers intercept and alter communication between devices.
- **Routing attacks:** Manipulating routing protocols can disrupt data flow and redirect traffic.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks:** Overwhelming the network with traffic to disrupt services.
- **Replay attacks:** Attackers capture and retransmit legitimate data to disrupt system operations.
- **Traffic sniffing and eavesdropping:** Attackers intercept sensitive data transmitted unencrypted over the network.

C. Application layer

The application layer, where data is processed and decisions are made, is also vulnerable to various types of attacks that can compromise the integrity and reliability of agricultural operations. Weak authentication mechanisms and poorly secured APIs can provide entry points for malicious actors to manipulate data, alter system configurations, or gain unauthorized access to sensitive information. Application-layer attacks include:

- **Unauthorized access:** Weak authentication mechanisms can allow unauthorized users to access sensitive data.
- **Command injection:** Attackers can alter or insert unauthorized commands to manipulate the system.
- **Data manipulation:** Attackers can tamper with stored data to disrupt operations.
- **API abuse:** Exploiting vulnerabilities in APIs can allow attackers to gain unauthorized access or manipulate data.

III. Intrusion Detection Systems

IDS have been proposed to capture attacks in Agriculture 4.0 that aim to detect specific layer attacks [5]. However, few have been used to detect anomalies due to faults and attacks for every layer. The rest of the section presents the techniques that are currently being used for the identification of unauthorized access.

A. Detection Models

The method of constructing a detection model depends both on the type of data available and on the location where the model is deployed (see Section III-B). In Agriculture 4.0, the diversity of sensors, data types, and environmental conditions requires a flexible and adaptive approach to the design of detection models.

A simple approach, such as setting static thresholds for identifying anomalies in sensor data, can often be misleading. Thresholds must be calibrated based on the environmental context and the physical location of the sensor, which may be subject to uncontrolled variables such as microclimate conditions or soil composition [9]. Furthermore, static thresholds are vulnerable to adversarial attacks, where an attacker slowly manipulates data over time to remain within the threshold bounds while causing significant system damage.

Binary Logistic Regression (BLR) has been shown to effectively identify anomalies using a minimal set of data characteristics (features), while maintaining high detection rates [6]. BLR is particularly useful for detecting binary outcomes, such as whether a sensor reading is anomalous or normal, based on a set of input features.

Beyond statistical methods, AI techniques are widely used for anomaly detection. These models are typically trained using historical data to construct a behavioral profile of the monitored environment, which is then used to predict and detect deviations. AI models can be broadly classified into supervised and unsupervised learning techniques. However, in Agriculture 4.0, the dynamic and unpredictable nature of environmental conditions can make it challenging to build accurate and reliable AI models.

In unsupervised learning, the model is trained only on data representing normal behavior (a single label). Any new, real-time data that significantly deviates from this trained profile is considered anomalous. While this approach does not require labeled attack data, a key limitation is its higher false positive rate when compared to supervised methods [10]. Unsupervised learning is particularly susceptible to environmental noise and natural variations in sensor data, leading to frequent false alarms.

Despite its limitations, unsupervised learning offers the advantage of not requiring datasets containing both normal and abnormal behavior. It builds a profile of what constitutes a ”normal” environment and flags anything outside that range. However, supervised learning models, when trained on both types of data, generally offer higher detection accuracy, especially for known attack types. A key challenge in supervised learning for Agriculture 4.0 is the scarcity of

labeled attack data, making it difficult to train models that generalize well to new and unseen attack scenarios.

One major challenge in deploying detection models is the need for customized training for each network or data environment. Insights gained from other systems can serve as guidelines, but variations in the physical setup, such as sensor placement and coverage, necessitate a context-specific approach. Furthermore, the dynamic nature of agricultural environments, with constantly changing conditions and evolving attack patterns, requires continuous model retraining and adaptation.

Another critical aspect is the validity and security of the training data. Training may be performed either offline or on the fly, but in both cases, the integrity of the training dataset must be ensured. If an attacker performs reconnaissance and determines that the model is being trained in real time, they could attempt a data poisoning attack—injecting malicious data during the training phase to manipulate the model into accepting abnormal inputs as normal [11]. Data poisoning attacks are particularly challenging to detect in Agriculture 4.0 due to the complexity of the environment and the potential for non-malicious data anomalies to mask malicious injections.

B. Location

The location of the detection model significantly influences the choice of tools and techniques used to implement it [7]. Resource-intensive detection models cannot be deployed at the perception layer, as many hardware devices at this level, such as Programmable Logic Controllers (PLCs), may lack the processing power or memory required to support them. Furthermore, the limited energy resources of many IoT devices in the perception layer necessitate lightweight detection models that minimize power consumption while maintaining acceptable detection accuracy. When WSNs are integrated into the perception layer, some devices may support lightweight detection models and function as local IDS agents [2], [6]. These local agents are capable of detecting anomalies or abnormal behavior in sensor readings or sensor malfunctions before data is transmitted to higher system layers. However, the limited processing power and memory of these local agents can restrict the complexity and effectiveness of the detection models they can support.

Drones are increasingly employed in smart agriculture for remote sensing and data collection. Ensuring the reliability and security of drone-generated data is critical, and equipping them with on-board detection mechanisms can help intercept tampering attempts early, preventing the propagation of compromised data through the system [12]. However, the computational and energy constraints of drones pose significant challenges to implementing effective on-board detection mechanisms.

In the network and application layers, IDS agents can be deployed in either centralized or decentralized configurations. Decentralized IDS agents can be positioned to collect data from multiple sources and collaboratively detect anomalies through distributed analysis. The same concept applies at the edge, where cooperative detection across nearby nodes can enhance early threat identification. Decentralized configurations offer improved scalability and resilience compared to centralized approaches but require careful coordination and communication between distributed agents.

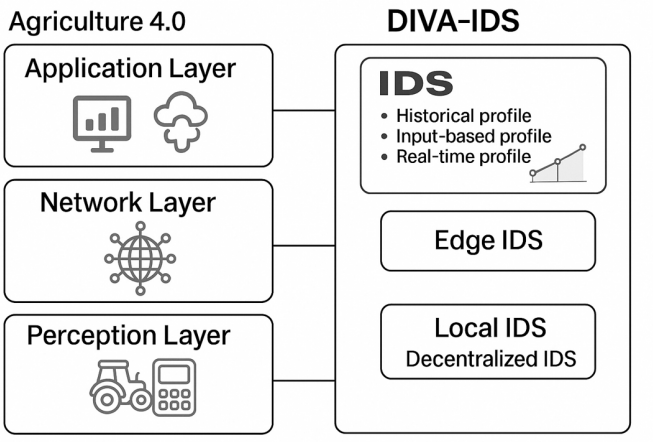

Fig. 1. DIVA-IDS framework: A cross-layer architecture for data integrity validation and anomaly detection in Agriculture 4.0.

The location of the IDS agent determines the type of data it receives as input. At the network layer, IDS agents typically monitor network traffic, focusing on packet flow, protocol behavior, and routing anomalies. At the application layer, IDS agents may analyze both sensor data readings and application-level traffic, providing a broader context for detecting malicious behavior or inconsistencies. However, relying on data from a single layer can limit the effectiveness of intrusion detection, as attackers may exploit vulnerabilities across multiple layers to evade detection.

IV. DIVA-IDS: A Cross-Layer Intrusion Detection and Validation Architecture

We propose DIVA-IDS (Data Integrity Validation and Anomaly Detection Intrusion Detection System), a cross-layer framework designed to ensure comprehensive coverage and robust data integrity assurance in Agriculture 4.0 environments (see Fig. 1). DIVA-IDS is not merely an intrusion detection system; it is a holistic security architecture that combines data validation, anomaly detection, and collaborative threat intelligence to address the unique challenges of modern agricultural systems.

A. Core Objectives and Design Principles

The primary objective of DIVA-IDS is to ensure that all automated or human decision-making processes within Agriculture 4.0 are based on reliable and trustworthy data. This objective extends beyond traditional security concerns to include the detection and mitigation of abnormalities caused by both malicious intent (such as cyberattacks) and physical or environmental faults (such as sensor degradation or interference). By providing timely detection and mitigation

capabilities, DIVA-IDS helps prevent further damage, enables the restoration of both network and agricultural operations to their intended state, and ensures the long-term resilience of smart farming systems.

Several key design principles guide the architecture and implementation of DIVA-IDS:

- **Cross-Layer Integration**: DIVA-IDS integrates detection and validation mechanisms across all layers of the Agriculture 4.0 architecture, from the physical sensors to the application-level analytics. This cross-layer approach enables the system to detect and respond to threats that may span multiple layers, providing a more comprehensive defense than traditional, layer-specific security solutions.
- **Data Integrity Validation**: DIVA-IDS incorporates mechanisms to validate the integrity of data at each layer of the system, ensuring that data has not been tampered with or corrupted. This validation process includes checks for data consistency, reasonableness, and provenance, as well as the use of cryptographic techniques to verify data authenticity.
- **Collaborative Anomaly Detection**: DIVA-IDS employs collaborative anomaly detection techniques to identify deviations from expected behavior across the system. These techniques leverage both historical data and real-time inputs to create behavioral profiles of sensors, network devices, and applications. Anomalies are detected by comparing current behavior against these profiles, with alerts generated for deviations that exceed predefined thresholds.
- **Resilience and Fault Tolerance**: DIVA-IDS is designed to operate without a single point of failure, ensuring that the system remains operational even in the event of component failures or attacks. This resilience is achieved through the use of decentralized architectures, redundant components, and automated failover mechanisms.

B. Layer-Specific Implementation Details

DIVA-IDS integrates detection mechanisms across all layers of the Agriculture 4.0 architecture, with layer-specific implementations tailored to the unique characteristics and vulnerabilities of each layer:

1) Perception Layer: At the perception layer, DIVA-IDS focuses on ensuring data integrity and detecting physical anomalies that may indicate sensor tampering or malfunction. In environments where WSNs are used, decentralized IDS agents can be deployed on sensor nodes to locally detect physical anomalies or low-level network-based attacks [6]. This localized approach improves resilience and enables early response. Specifically, these agents can:

- **Validate Sensor Readings**: Implement sanity checks to ensure that sensor readings fall within expected ranges and are consistent with physical constraints.
- **Detect Physical Tampering**: Monitor for physical disturbances or unauthorized access to sensor devices.
- **Analyze Communication Patterns**: Identify abnormal communication patterns that may indicate a compromised sensor node.

2) Network Layer: At the network layer, DIVA-IDS agents monitor traffic to detect attacks such as routing manipulation, packet injection, or denial of service. These agents analyze communication metadata to uncover abnormal patterns that may indicate an ongoing or emerging threat [13]. Key capabilities at this layer include:

- **Traffic Analysis**: Monitor network traffic for anomalies, such as unusual packet sizes, protocols, or destinations.
- **Routing Integrity**: Validate the integrity of routing protocols to detect manipulation or redirection of traffic.
- **Denial-of-Service Detection**: Identify and mitigate DoS/DDoS attacks by analyzing traffic patterns and blocking malicious sources.

Furthermore, DIVA-IDS employs techniques such as deep packet inspection (DPI) to analyze the content of network packets and detect malicious payloads or command injections.

3) Application Layer: At the application layer, DIVA-IDS performs higher-level data analysis, integrating data from various sources to create a comprehensive view of the agricultural environment. Here, sensor data profiles are created over time and used in combination with AI-based models, either supervised or unsupervised, to detect known and unknown attacks. For instance, if the system maintains historical data and also receives contextual input such as fertilization records or irrigation schedules, it can make informed predictions about expected sensor behavior. When real-time data deviates significantly from those predictions, it may indicate the presence of a compromised sensor or injected false readings. The application layer is equipped with mechanisms to:

- **Analyze Sensor Data Profiles**: Create and maintain profiles of expected sensor behavior based on historical data and contextual inputs.
- **Detect Anomalies**: Use AI-based models to detect deviations from expected behavior, indicating potential attacks or faults.
- **Correlate Data Across Layers**: Integrate data from multiple layers to identify cross-layer attacks or anomalies that may not be apparent at a single layer.

In addition to raw sensor readings, DIVA-IDS considers contextual environmental variables such as weather conditions, time of day, seasonal cycles, and manually recorded activities. All of these factors can influence expected outcomes. This fusion of operational and contextual data helps the system build more accurate and holistic profiles capable of detecting complex anomalies.

C. Cross-Layer Coordination and Collaborative Threat Intelligence

A key feature of DIVA-IDS is its ability to coordinate detection and response activities across multiple layers of the Agriculture 4.0 architecture. This cross-layer coordination enables the system to:

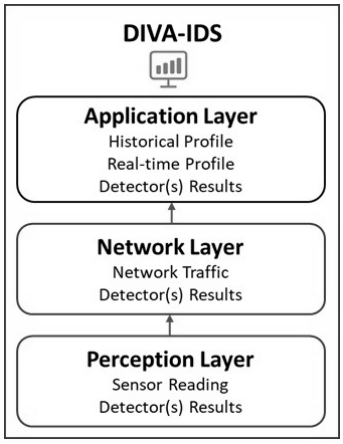

Fig. 2. DIVA-IDS System Flow

- **Share Threat Intelligence**: Exchange threat intelligence data between layers to improve detection accuracy and reduce false positives.
- **Orchestrate Responses**: Coordinate response actions across layers to mitigate the impact of attacks and restore system operations.
- **Adapt to Changing Conditions**: Dynamically adjust detection parameters and response strategies based on real-time conditions and threat intelligence.

Each layer in the system incorporates at least one dedicated anomaly detection component. These detectors can be implemented locally-installed directly on individual devices-or in a decentralized manner, collaboratively monitoring a segment or the entire network. This design ensures that all devices within the architecture are subject to continuous monitoring, regardless of their position or function.

The outputs generated by these anomaly detectors, whether related to sensor readings or network traffic, must be communicated to the application layer. The application layer is uniquely positioned to aggregate, interpret, and present these results to the end user in a meaningful and actionable format (see Fig.2).

There are three primary strategies for transmitting anomaly detection results: (a) utilizing the existing network infrastructure, (b) employing a dedicated communication channel, or (c) adopting a hybrid approach. Leveraging the existing network infrastructure is cost-effective compared to deploying a separate communication channel; however, it introduces risks of data loss or transmission delays, especially in the presence of DoS/DDoS attacks or other network-layer disruptions. While a dedicated channel can reliably transmit data to the application layer-unless it is directly targeted by an attack-it still remains susceptible to network disruptions. In contrast, a hybrid communication solution enhances system robustness by reducing single points of failure and ensuring that anomaly reports are delivered reliably to their destination.

By correlating inputs across multiple layers and integrating detection logic with both historical and real-time behavioral profiles, DIVA-IDS offers a comprehensive, distributed, and intelligent intrusion detection strategy tailored to the unique challenges of smart agriculture systems. This proactive and adaptive approach is essential for maintaining the security, reliability, and trustworthiness of Agriculture 4.0 in the face of evolving cyber threats and operational challenges.

V. Remarks and Conclusion

Agriculture 4.0 integrates advanced technologies to enhance productivity across the agricultural sector by enabling informed, timely decisions that help avoid losses and inefficiencies. Reliable, real-time data plays a crucial role in this decision-making process. However, even when data are encrypted, threats that compromise data integrity remain a significant concern. These include unauthorized modifications to sensor readings, denial of data transmission, or the injection of false information, all of which can lead to flawed decision-making and reduced productivity.

Early detection of such threats is essential to prevent irreversible damage caused by decisions based on compromised data. To address this challenge, DIVA-IDS introduces a cross-layer intrusion detection framework capable of identifying data anomalies across different system levels. The framework utilizes historical profiles, user and environmental input, and real-time data to detect inconsistencies that may indicate malicious activity or system faults. By integrating data integrity validation with collaborative anomaly detection, DIVA-IDS offers a more comprehensive and robust defense against the diverse threats facing Agriculture 4.0 systems.

The limitations of traditional, siloed security solutions in Agriculture 4.0 highlight the critical need for a cross-layer approach like DIVA-IDS. Traditional solutions often focus on specific layers or threat types, neglecting the systemic risks posed by cross-layer attacks and the potential for data corruption due to both malicious and non-malicious causes. DIVA-IDS addresses this gap by providing a unified approach to intrusion detection across all layers of the Agriculture 4.0 architecture. This cross-layer integration allows the system to correlate inputs from different layers, share threat intelligence, orchestrate responses, and dynamically adapt to changing conditions and evolving threat landscapes.

While building and maintaining such profiles requires additional computational and memory resources, the benefits outweigh the costs. In particular, they enhance trust in data and support precision-based agricultural decisions, ultimately contributing to greater resilience and productivity in Agriculture 4.0 systems. Furthermore, the ability to distinguish between malicious intrusions and data anomalies caused by non-malicious factors allows for more targeted and effective responses, minimizing disruptions and maximizing the efficiency of agricultural operations. The need for such a cross-layer framework becomes even more pronounced as Agriculture 4.0 systems become more complex and interconnected, increasing the potential for cascading failures and sophisticated attacks.

Future research directions include the development of adaptive anomaly detection models that can automatically adjust to changing environmental conditions and evolving threat landscapes. Additionally, the integration of blockchain technology for secure data provenance and tamper-proof audit trails could further enhance the trustworthiness and reliability of Agriculture 4.0 systems. Finally, field testing and real-world deployment of the DIVA-IDS framework are needed to validate its effectiveness and identify potential areas for improvement.

In conclusion, DIVA-IDS represents a significant step forward in securing Agriculture 4.0 systems by providing a cross-layer intrusion detection and validation architecture that addresses both malicious and non-malicious threats. By ensuring data integrity and promoting collaborative anomaly detection, DIVA-IDS can help unlock the full potential of Agriculture 4.0, enabling more efficient, sustainable, and resilient agricultural practices.

REFERENCES

[1] V. Kumar, K. V. Sharma, N. Kedam, A. Patel, T. R. Kate, and U. Rathnayake, "A comprehensive review on smart and sustainable agriculture using iot technologies," *Smart Agricultural Technology*, vol. 8, p. 100487, 2024.

[2] M. Catelani, L. Ciani, A. Bartolini, C. Del Rio, G. Guidi, and G. Patrizi, "Reliability analysis of wireless sensor network for smart farming applications," *Sensors*, vol. 21, no. 22, 2021.

[3] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Applied Sciences*, vol. 11, no. 16, 2021.

[4] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[5] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 407–436, 2021.

[6] C. Ioannou, V. Vassiliou, and C. Sergiou, "An intrusion detection system for wireless sensor networks," in *2017 24th International Conference on Telecommunications (ICT)*, 2017, pp. 1–5.

[7] C. Ioannou and V. Vassiliou, "Security agent location in the internet of things," *IEEE Access*, vol. 7, pp. 95 844–95 856, 2019.

[8] R. Ahmad and I. Alsmadi, "Machine learning approaches to iot security: A systematic literature review," *Internet of Things*, vol. 14, p. 100365, 2021.

[9] C. Charilaou, C. I. Ioannou, and V. Vassiliou, "System for operational technology attack detection in industrial iot," in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2022, pp. 84–93.

[10] C. Ioannou and V. Vassiliou, "Network attack classification in iot using support vector machines," *Journal of Sensor and Actuator Networks*, vol. 10, no. 3, 2021.

[11] M. Goldblum, D. Tsipras, C. Xie, X. Chen, A. Schwarzschild, D. Song, A. Madry, B. Li, and T. Goldstein, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 2, pp. 1563–1580, 2023.

[12] K. Aslansefat, P. Nikolaou, M. Walker, M. N. Akram, I. Sorokos, J. Reich, P. Kolios, M. K. Michael, T. Theocharides, G. Ellinas, D. Schneider, and Y. Papadopoulos, "Safedrones: Real-time reliability evaluation of uavs using executable digital dependable identities." Berlin, Heidelberg: Springer-Verlag, 2022, p. 252–266. [Online]. Available: https://doi.org/10.1007/978-3-031-15842-1_18

[13] C. Ioannou and V. Vassiliou, "Experimentation with local intrusion detection in iot networks using supervised learning," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2020, pp. 423–428.