SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I1P112

Volume 11 Issue 1, 150-161, January 2024
© 2024 Seventh Sense Research Group®

Original Article

Energy-Efficient X-Layer Intrusion Detection System for Agriculture Atmosphere Monitoring Using Wireless Sensor Networks

S. Helga Selvin[1], A. Devi[2]

[1]Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science (Autonomous), Tamilnadu, India.
[2]Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts and Science (Autonomous), Tamilnadu, India.

[1]Corresponding Author : arunhelga@gmail.com

Received: 19 October 2023 Revised: 29 November 2023 Accepted: 20 December 2023 Published: 13 January 2024

Abstract *- In modern agriculture, monitoring and maintaining optimal atmospheric conditions are critical for crop health and productivity. Wireless Sensor Networks (WSNs) have emerged as a valuable technology for collecting real-time data from agricultural environments. However, deploying WSNs in agriculture exposes them to security threats, making intrusion detection essential. We propose an Energy-Sensitive Clustering algorithm with an X-Layer Intrusion Detection System (XL-IDS) tailored for agriculture atmosphere monitoring using WSNs to address this challenge. Our IDS leverages the unique characteristics of WSNs and employs an X-layer approach to enhance detection accuracy while minimizing energy consumption. The system monitors WSN protocol stack layers, including the physical, data connection, network, and application layers, to identify and mitigate intrusions effectively. Our system employs clustering algorithms to optimize energy usage to organize sensor nodes efficiently. This reduces the communication overhead and extends the network's lifetime. The IDS model provides real-time alerts to farmers and agricultural operators, allowing them to take immediate action when security threats or anomalies are detected, thereby safeguarding the data and the crops.*

Keywords *- Wireless Sensor Network, Precision agriculture, X-Layer Intrusion Detection System, Atmosphere monitoring, Energy-sensitive clustering.*

1. Introduction

Agriculture has endured a remarkable transition in recent years, propelled by technological developments ushered in the era of precision agriculture. In this new paradigm, farmers and growers harness data-driven insights to optimize crop yields, reduce resource waste, and ensure food security for an ever-growing global population [1]. WSNs have emerged as a pivotal technology in this transformation, enabling real-time data collection from agricultural environments [2]. These networks, composed of numerous tiny sensor nodes, provide critical information about soil conditions, weather patterns, and atmospheric parameters to help farmers make informed decisions [3].

However, the proliferation of WSNs in agriculture has introduced a new dimension of concern - security [4]. As the number of deployed sensor nodes increases and these nodes become increasingly interconnected, they become vulnerable to various security threats. Unauthorized access, data tampering, and disruption of network services can jeopardize the integrity of collected data and crops' overall health and productivity [5].

In this context, IDS have become indispensable tools for safeguarding agricultural sensor networks [6]. Traditional IDS solutions designed for conventional networks may not directly apply to the unique characteristics and constraints of WSNs [7, 8]. Wireless sensor nodes are resource-constrained, operate on limited battery power, and are often deployed in remote and harsh environments [9]. Consequently, there is a pressing need for energy-efficient and context-aware intrusion detection mechanisms specifically tailored for agriculture atmosphere monitoring using WSNs [10].

This paper introduces an innovative Energy-Efficient XL-IDS designed explicitly for the unique challenges posed by agriculture atmosphere monitoring using Wireless Sensor Networks. Our XL-IDS not only enhances the security of WSNs in agricultural settings but also optimizes energy consumption, extending the operational lifetime of sensor nodes and improving the sustainability of precision agriculture. In the following sections, we will explore the design, implementation, and evaluation of our proposed XL-IDS. We will explore the X-layer approach that integrates insights from various protocol layers to enhance intrusion detection accuracy. Additionally, we will discuss the energy-aware clustering mechanisms employed to reduce communication overhead and improve network longevity. Real-world deployment scenarios and performance evaluations will demonstrate the effectiveness and practicality of our energy-efficient XL-IDS in ensuring the security and reliability of agriculture atmosphere monitoring systems.

In agriculture atmosphere monitoring, the implementation of IDS using WSN plays a pivotal role in ensuring the integrity and reliability of data gathered from agricultural environments. However, despite advancements in this field, a noticeable research gap persists in developing an energy-efficient X-Layer IDS tailored specifically for agriculture atmosphere monitoring. Given the resource-constrained nature of sensor nodes deployed in vast agricultural landscapes, this gap arises from the need to enhance energy use efficiency in WSNs.

This research addresses the identified gap by introducing a novel Energy-Efficient X-Layer Intrusion Detection System designed explicitly for agriculture atmosphere monitoring. The fundamental motivation behind this work is to enhance the sustainability and longevity of WSNs in agricultural settings, where traditional intrusion detection systems may fall short due to their energy-intensive nature.

2. Related Works

IDS may be used with wireless sensors to identify intrusions in farm fields and deliver an alarm message to the user. The system is built on the Message Queue Telemetry Transport protocol [11], which allows information to be sent between internet-connected devices. The globe is facing a significant obstacle in the form of a lack of fresh water, and it is expected that this predicament will become much direr in the years to come. Because of the difficulties described above, intelligent irrigation and precision farming are the only alternatives likely to be successful. This article [12] outlines a methodology for identifying and categorizing intrusions into the Internet of Things networks used in agricultural settings.

This article suggested a Federated Learning-based Intrusion Detection System (FELIDS) to protect agricultural Internet of Things infrastructures [13]. To be more specific, the FELIDS system safeguards data privacy via the process of local learning. In this method, devices get an advantage from the collective wisdom of their contemporaries and only share model updates with an aggregate server, which ultimately results in an enhanced detection model. An Intrusion Detection System (IDS) model was developed in this study [14]. It uses a deep learning method, a conditionally generative adversarial network, and the addition of an XGBoost classifier for quicker comparison and visualization of findings.

Because attack scenarios have evolved, finding a practical and ideal network IDS that receives regular updates has become difficult. This is the reason why this article [15] pulls together publically accessible intrusion datasets and Machine-Learning approaches that have been used in recent intrusion detection systems to illustrate both present-day issues and potential prospects.

To solve the deficiencies of current WSNs regarding energy efficiency, our suggested model incorporates high-performance information that offers a platform for WSNs to assist agricultural output better. This is done to overcome the weaknesses of existing WSNs. This research [16] demonstrates the benefits of the suggested method over previous strategies in conserving energy in WSN and in monitoring the process of conserving water.

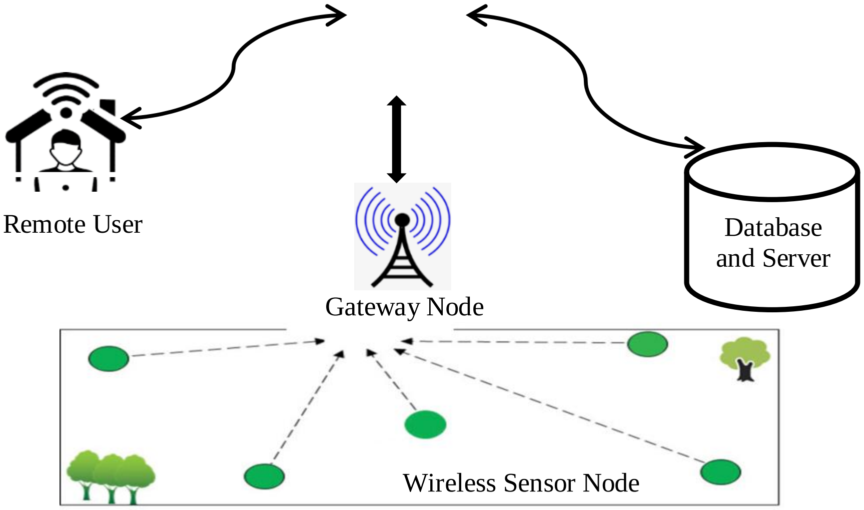


Fig. 1 Agricultural field with WSN

The authors of this study [17] use advanced image recognition algorithms in intelligent sensor networks to thoroughly examine and analyze the environmental profitability of precision farming. Their discoveries can be discovered in the subsequent sentences. Filtering and thresholding convert the analog signal generated from the wireless sensor network into a digital signal. This phase is essential for completing the data preparation for sensor monitoring before doing digital information analysis. Industry 4.0 can generate a novel revolution by offering smart, safe, self-sufficient, and adaptable networks. Internet of Things nodes may be grouped using a clustering technique to form clusters, enhancing networks' efficiency, durability, and stability [18].

IoT sensors enable farmers to remotely regulate their crops and agricultural fields, opening up new possibilities for precision agriculture. Recent studies have focused on improving the safety and protection offered by precision agriculture [19]. A situational or dynamic security approach must have a secure Internet of Things network.

Adaptive security, a cybersecurity-based strategy, is one advanced security solution that can improve the security of the Internet of Things [20]. Agriculture is the most important factor in maintaining global equilibrium; with the help of precision farming, Internet of Things smart agri-sensors, and other intelligent approaches, food production is continuous and balanced. If these cutting-edge technologies are subjected to intrusion assaults, the equilibrium may be upset; to avoid these problems, an IDS is required to guarantee security and privacy to wireless sensor networks [21]. The Internet of Things is relevant to many application areas, such as the smart grid, agriculture, and medical care. The goal of this article [22] is to give a thorough survey on the function of IoT in the livestock industry by classifying and synthesizing previous research work done in this area. The survey will be presented in the form of an article. These two technologies are ushering in a new age of precision agriculture, replacing traditional farming methods. This study [23] aims to use IoT and UAV technologies in agricultural settings.

The research introduced the Automated Machine Learning model [24] to provide intrusion detection and prevention techniques. Cyberattacks can turn off the operation of Internet of Things apps entirely. With Artificial Intelligence and, more specifically, deep learning algorithms, the authors of this research [25] investigate the risks associated with using intelligent agricultural applications.

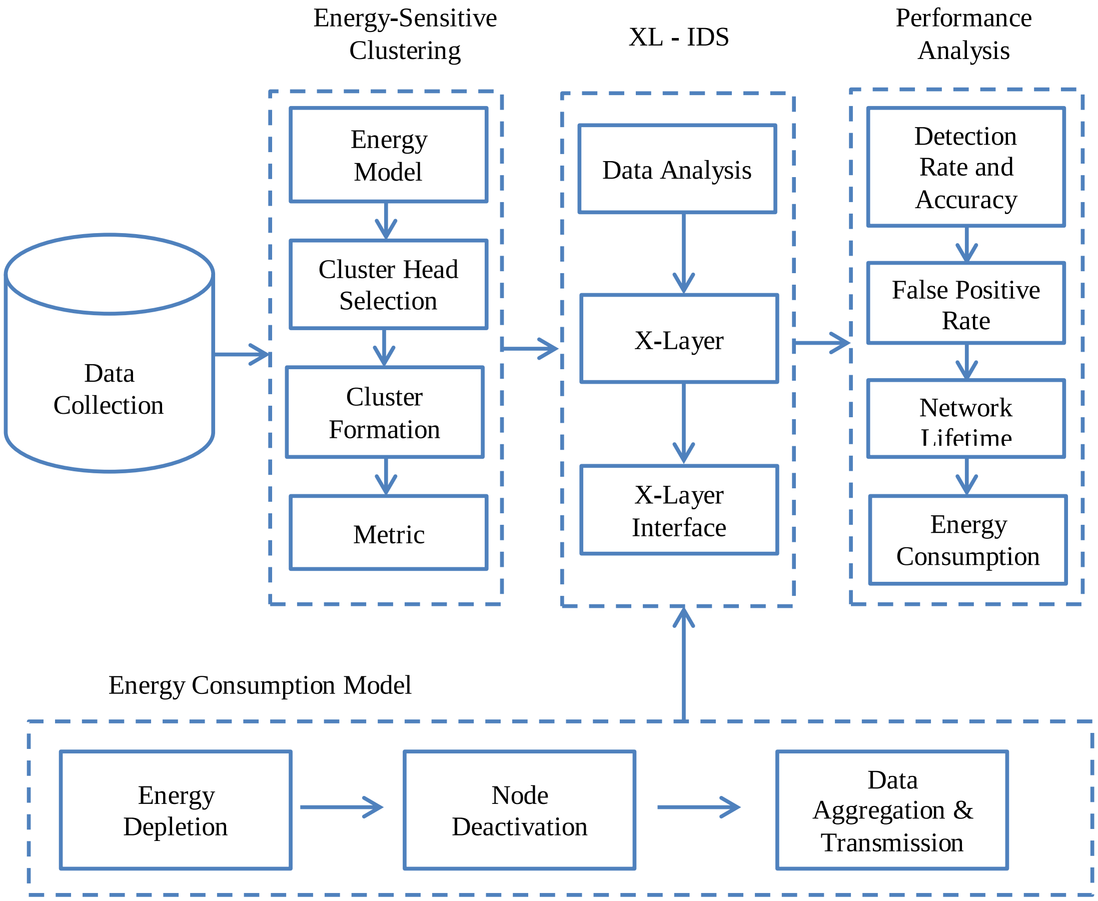


Fig. 2 Overall agriculture for energy-sensitive clustering and XL-IDS for WSN

Existing research predominantly focuses on general intrusion detection systems and their application in diverse environments, with limited attention given to the unique challenges of agriculture settings. While studies have explored using WSNs for intrusion detection, few have explicitly addressed the energy constraints inherent in agriculture-specific deployments. This research fills this gap by proposing an energy-efficient X-Layer Intrusion Detection System, recognizing sensor nodes' distinct energy challenges in expansive agricultural landscapes.

However, energy efficiency is a critical consideration in the design and operation of IDS for agriculture atmosphere monitoring using WSN. This may be overcome by optimizing the WSN's energy consumption to prolong the lifespan of the sensors and minimize maintenance requirements by energy-efficient routing protocols.

3. Proposed Model

Our proposed model is designed to discuss the challenges and requirements of securing WSNs in agricultural environments while optimizing energy consumption. Sensor nodes are the low-power sensor devices deployed throughout the agricultural field responsible for collecting environmental data.

Each sensor node is equipped with sensors for monitoring various atmospheric parameters such as temperature, humidity, and gas concentrations. Sensor nodes are organized into clusters to optimize energy consumption by implementing an Energy-Sensitive Clustering algorithm. Cluster Heads (CH) are responsible for aggregating data from member nodes, processing initial data, and relaying information to the Base Station (BS).

Cluster-based network topologies are commonly used in various networks to improve efficiency, scalability, and manageability. BS collects data from cluster heads, processes intrusion detection information, and communicates with the external world, including notifying farmers or operators of security incidents.

Cluster heads are liable for gathering and forwarding data to the BS, reducing energy-intensive long-distance communication. We integrated energy-sensitive clustering with the XL-IDS Model. It operates at multiple protocol layers, including the physical, data link, network, and application layers, enabling cross-layer analysis for intrusion detection. The IDS employs anomaly detection techniques to identify deviations from expected behavior and intrusion patterns. Our proposed IDS provides real-time alerts to farmers or operators when an intrusion or anomaly is detected.

Mathematical model for energy-aware clustering

Notation:
N - The total amount of sensor nodes that are part of the network.
D - Diameter of the sensor field (maximum distance between any two nodes).
T - Time slots of monitoring window.
$E_i(t)$ - Energy level of sensor node i at time t.
E_{max} - Maximum energy volume of a sensor node.
E_{th} - Energy threshold for node operation.
R - Radius for cluster formation.
$C_i(t)$ - Cluster head selection probability for node i at time t.
S - Set of sensor nodes.
M - Number of cluster head nodes.
CH - Set of cluster head nodes.
NCH - Set of non-cluster head nodes.
T_{CH} - Time for cluster head selection.
D_{ij} - Distance between nodes i and j.
W - Set of neighboring nodes within radius R of node i.
P_i - Power consumption of sensor node i in a given time slot.
D_i - Data transmission rate of sensor node i.
L - Number of protocol layers analyzed by the IDS.
R - Detection rate of the IDS.
F - False positive rate of the IDS.
C - Communication overhead in bits.
I - Number of detected intrusions.
T_{data} - Time taken to transmit data to the Base Station.
T_{total} - Total time for IDS operation.
W - Window size for cross-layer analysis.

3.1. Energy Model

3.1.1. Energy Consumption in Transmitting Data

$$P_{tx} = \frac{E_{tx}}{E_{elec}} . d^2$$

The energy used up to transmit a bit of information over a distance *d*, where E_{tx} is the energy required to communicate a bit and E_{elec} is the energy required to run the radio.

3.1.2. Energy Consumption in Receiving Data

$$P_{rx} = \frac{E_{rx}}{E_{elec}}$$

The energy consumed to receive a bit of data where E_{rx} is the energy required to receive a bit.

3.2. Cluster Head Selection

3.2.1. Cluster Head Selection Probability

$$C_i(t) = \frac{E_i(t)}{E_{max}} . \left(1 - \frac{E_i(t)}{E_{th}}\right) . \frac{1}{|W|}$$

The Probability of node *I* becoming a cluster head to time *t* is based on its energy level, energy threshold, and the number of neighboring nodes within radius *R*.

3.3. Cluster Formation

3.3.1. Cluster Formation Criterion

- Node *i* becomes a cluster head at time *t* if $C_i(t) > C_j(t)$ for all j $\in$ W.
- The node with the highest cluster head selection probability in its neighbourhood becomes the cluster head.

3.3.2. Number of Cluster Heads

$$|CH| = \sum_{i \in S} \delta_i(t)$$

The total number of cluster heads is the sum of the indicator variables. $\delta_i(t)$ representing whether node i becomes a cluster head at time *t*.

3.4. Energy-Efficiency Metric

Energy - efficiency metric for Clustering measures the ratio of the number of cluster heads to the total energy consumed for communication.

$$\text{Energy} - \text{Efficiency} = \frac{|CH|}{\sum_{i \in S}(P_{tx} + P_{rx})}$$

The above mathematical model provides a framework for the Energy-Sensitive Clustering algorithm’s key components and contribution of energy-efficient cluster formation in WSNs.

3.5. XL-IDS

XL-IDS are the component that facilitates communication between the various levels and apps. It basically consists of two components: the interaction interface and the X-layer Interface. The interaction interface facilitates communication between the layers and applications and the X-Layer system.

These methodologies are used to obtain or refresh data. The framework for XL-IDS is illustrated in Figure 3. In this framework, a Sensor Node (SN) monitors its neighbor node by estimating the trust value at each layer, such as physical, MAC, and network. Several attacks are primarily directed against the network layer, which is used for data routing in the network. Hence, the system only considers these three layers for estimating an SN’s final reliability. First, the trust parameters are selected to compute the trust at every layer. The trust parameters pertaining to the physical layer include the energy dissipation of an SN and the quantity of messages received from such SN. The trust parameters at the MAC layer include the back-off time and the count of successfully executed transmissions. The trust parameters pertaining to the network layer include the specified number of hops. The suggested IDS utilizes an X-layer design that leverages the interaction and cooperation of three contiguous levels within the OSI model: the network, Mac, and physical layers. As seen in Figure 4, the measured signal intensity for a wireless medium directly correlates with the spatial separation of nodes. The fundamental concept behind our IDS is identifying unauthorized individuals when they attempt to communicate with the various nodes within the network. After receiving RTS packets from the invading node, the detection method examines if the targeted node is a neighbouring node in the routing path.

Consequently, if a node is excluded from the routing path and attempts to establish communication by receiving RTS packets from the sensor nodes, it is promptly recognized as an unauthorized entity. In the absence of explicit authentication via RSSI, it becomes challenging to ascertain the true origin of a packet received by a node. TinyOS, an emerging embedded operating system, has been designed with the functionality to get the Received Signal Strength Indicator (RSSI) value. Integrating the Received Signal Strength Indicator (RSSI) value with the neighbourhood routing database significantly enhances the detection capability.

3.6. Energy Consumption Model

3.6.1. Energy Consumption in Data Transmission

$$Pi(t) = Di \cdot Ei(t)$$

Energy consumption of sensor node i in a given time slot is proportional to its data transmission rate and current energy level.

Energy Depletion

$$Ei(t+1) = Ei(t) - Pi(t)$$

The energy level of sensor node i decreases over time due to power consumption.

Node Deactivation

Sensor nodes with energy levels below a threshold Eth deactivate and stop participating in network operations.

3.7. Intrusion Detection Model

Figure 5 provides a comprehensive overview of the various options available for evaluating the legitimacy of a node. In due course, the proposed algorithm is anticipated to result in a higher proportion of accurate positive and negative outcomes while reducing the proportion of erroneous positive and negative outcomes.

3.7.1. Cross-Layer Analysis

$$IDS_{CL} = IDS_{PH} \cap IDS_{DL} \cap IDS_{NL} \cap IDS_{AL}$$

The Intrusion Detection System’s output at each protocol layer is combined through logical intersection to generate a cross-layer intrusion detection result.

Detection Rate and False Positive Rate

$$R = \frac{I}{I_{total}}$$

$$F = \frac{FP}{I_{total}}$$

Detection and false positive rates are calculated based on the number of detected intrusions (I) and total intrusions (I_{total}).

3.8. Network Operation Model

Energy-Sensitive Clustering: The energy-efficient clustering algorithm selects cluster heads that minimize energy consumption for data aggregation and transmission.

$$C = \sum_{i=1}^{N} C_i$$

Total communication overhead is the sum of communication overhead for each sensor node.

Network Lifetime: The network lifetime is determined by the time at which the first sensor node deactivates.

$$Network\ Lifetime\ = min_i \left(\frac{E_i(0)}{P_i}\right)$$

It is the minimum time among all sensor nodes depletion times.

3.8.1. Energy – Efficiency Metric

$$Energy - Efficiency = \frac{Total\ Data\ Sent}{Total\ Energy\ Consumed}$$

It measures the amount of data sent per unit of energy consumed. Maximizing energy efficiency is essential to prolong the lifespan of the sensors, minimize maintenance requirements, and reduce overall operational costs. Reduce the frequency of data collection to the minimum required for accurate monitoring while ensuring that essential events or anomalies are captured.

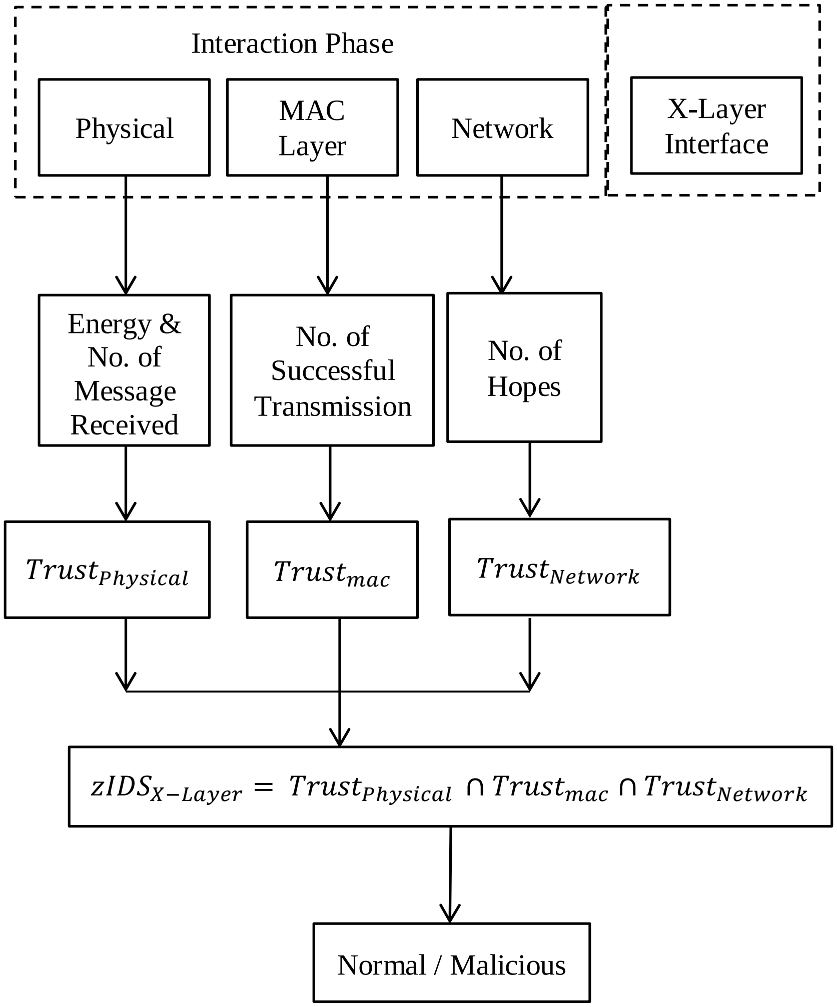


Fig. 3 Proposed XL-IDS model

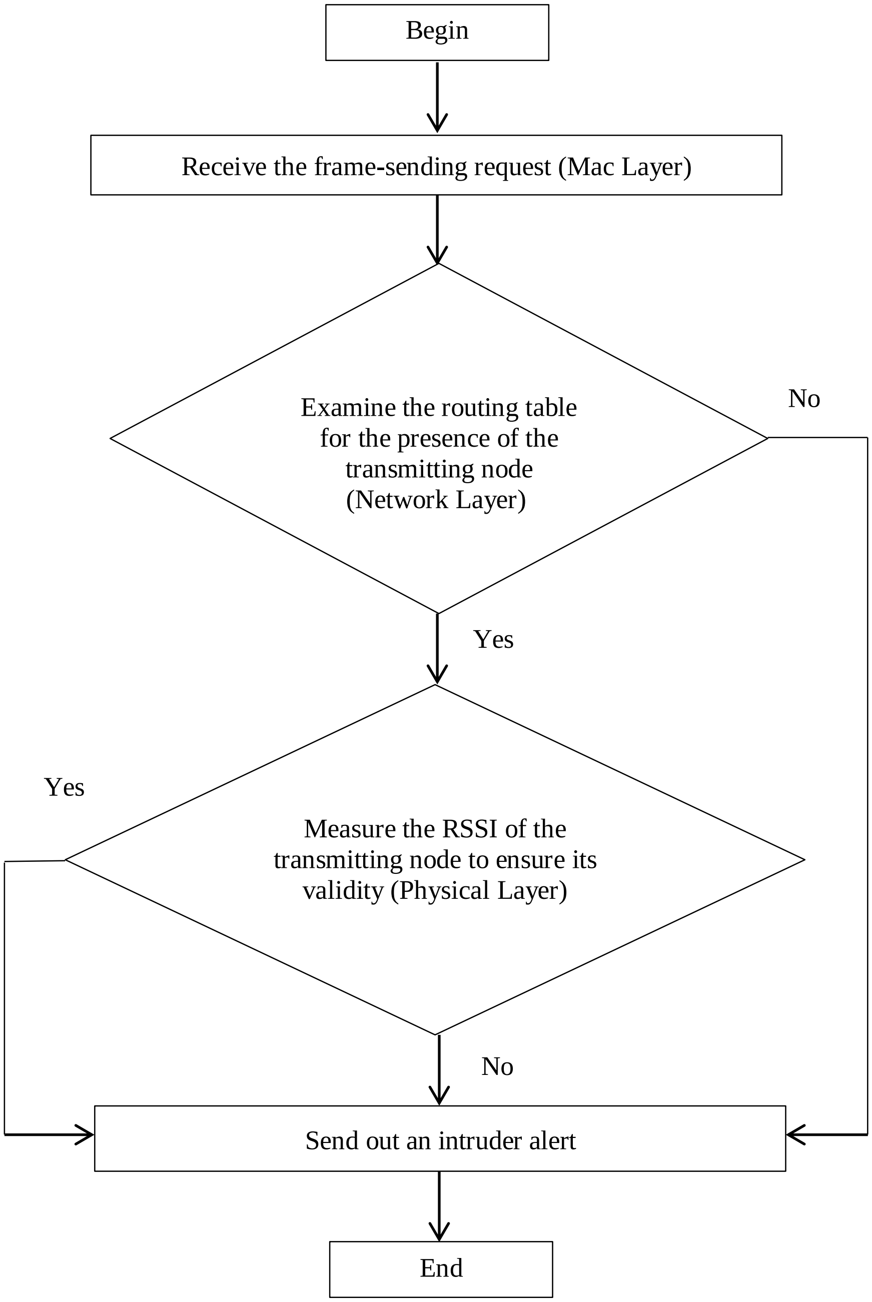
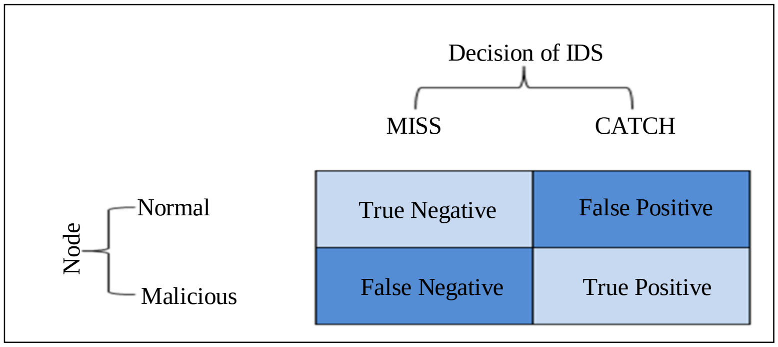

Begin
Receive the frame-sending request (Mac Layer)
Examine the routing table for the presence of the transmitting node (Network Layer)
No
Yes
Measure the RSSI of the transmitting node to ensure its validity (Physical Layer)
Yes
No
Send out an intruder alert
End

Fig. 4 Proposed XL-IDS model



	MISS	CATCH
Normal	True Negative	False Positive
Malicious	False Negative	True Positive

Fig. 5 All possible detection results of IDS

4. Results and Discussions

Evaluation of the efficacy of our system for intrusion detection is conducted with the network simulator NS2. The simulation employs an experimental model of 100 randomly dispersed nodes on a square area of 100 × 100 m², as seen in Figure 6. Table 1 presents a comparative analysis of the accuracy of the proposed frameworks and current approaches in identifying IDS in WSN.

Figure 7 shows that the detection accuracy of the proposed Energy Efficient XL-IDS is better than the existing methods. The proposed Energy Efficient XL-IDS produces a higher detection accuracy of 95.43%, whereas the CIDS method metric is 94.21%, and the Auto-IDS method metric is 93.6%, higher than other existing models. The proposed method produces better detection accuracy than the current security methods. Table 2 presents a comparative analysis of the detection rate achieved by the suggested technique in contrast to standard methods. The results demonstrate that the proposed methodology attains a detection rate of 95.2% when confronted with a single attacker. The system's scalability is shown by its capacity to achieve a detection rate of 94.2% when the number of attackers was raised to 10, as seen in Figure 8.

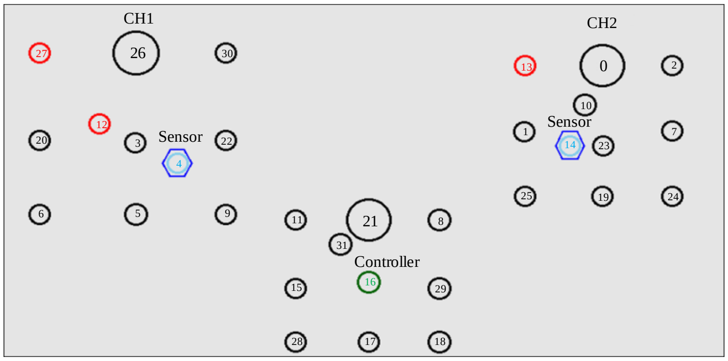


Fig. 6 Experimentation model

Table 1. Comparison of detection accuracy

Authors	Methods	Detection Accuracy
Anand et al. [19]	AgroKy	85.27
Sood et al. [14]	Conditional IDS	90.43
Chakravarthy et al. [11]	MQTT	91.6
Friha et. al [13]	FELIDS	93.4
Singh et al. [24]	Auto-IDS	93.6
Mansour et al. [18]	CIDS	94.21
Proposed Model	Energy Efficient XL-IDS	95.43

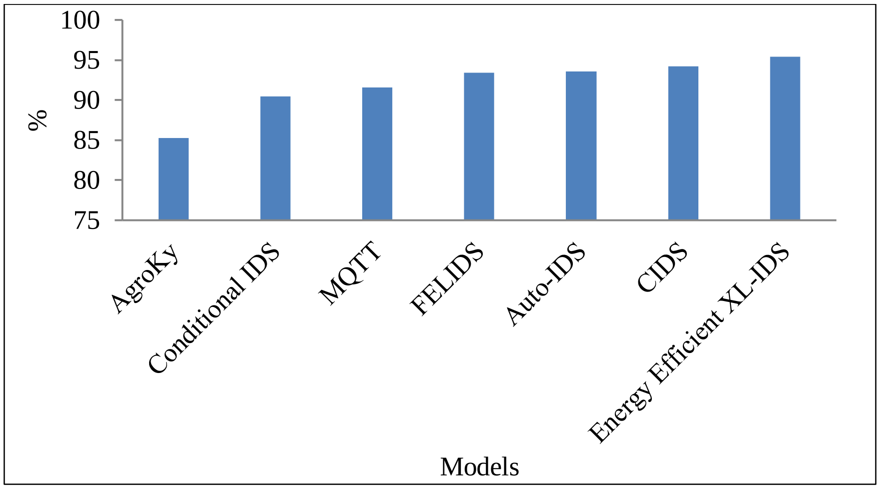


Fig. 7 Detection accuracy comparison between proposed and existing models

Table 2. Comparison of detection rate

Number of Attackers	AgroKy	Conditional IDS	MQTT	FELIDS	Auto-IDS	CIDS	Energy Efficient XL-IDS
1	91.3	92.86	93.72	93.99	94.98	94.86	95.2
2	91.2	92.68	93.65	93.89	94.92	94.80	95.12
3	91.16	92.45	93.15	93.86	94.89	94.6	95.02
4	91.1	91.99	92.84	93.86	94.79	94.56	94.98
5	90.98	91.75	92.74	93.81	94.67	94.32	94.68
6	90.87	91.63	92.63	93.78	94.56	94.23	94.65
7	90.63	91.6	92.55	93.72	94.12	94.17	94.35
8	90.51	91.59	92.5	93.65	93.98	94.15	94.21
9	90.43	91.38	92.45	93.65	93.9	94.04	94.05
10	90.12	91.15	92	93.62	93.72	94.01	94.02

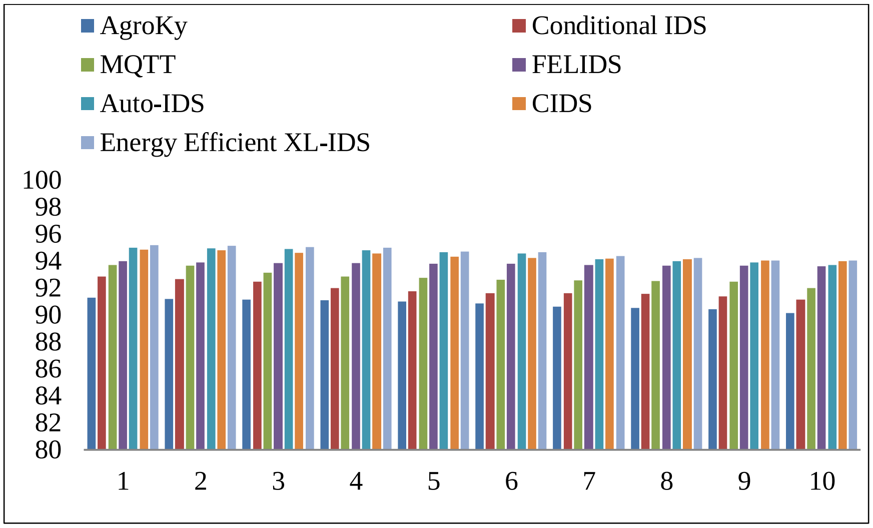


Fig. 8 Comparison of detection rate

Table 3 presents a comparative analysis of the False Positive Rate (FPR) between the proposed model and existing techniques. The findings indicate that the proposed model yields a false positive rate of 0.01 when confronted with a single attacker. The scalability of the method is demonstrated by achieving a detection rate of 0.09% when the number of attackers was increased to 10, as illustrated in Figure 9. Table 4 presents a comparative analysis of energy consumption between the proposed method and conventional methodologies.

The process under consideration demonstrates an energy consumption of 1294.35 mJ over a simulation duration of 100 seconds. The proposed method in this study resulted in an energy consumption of 1194.64 mJ over a simulation time of 500 seconds, as depicted in Figure 10.

Table 3. Comparison of false positive rate

Number of Attackers	AgroKy	Conditional IDS	MQTT	FELIDS	Auto-IDS	CIDS	Energy Efficient XL-IDS
1	0.1	0.14	0.1	0.05	0.08	0.01	0.01
2	0.16	0.17	0.17	0.09	0.1	0.04	0.01
3	0.18	0.21	0.18	0.12	0.11	0.06	0.02
4	0.23	0.27	0.21	0.15	0.15	0.07	0.03
5	0.27	0.31	0.25	0.18	0.17	0.07	0.03
6	0.36	0.37	0.3	0.2	0.19	0.09	0.05
7	0.48	0.41	0.31	0.21	0.24	0.1	0.05
8	0.52	0.46	0.38	0.25	0.25	0.12	0.06
9	0.58	0.52	0.41	0.29	0.27	0.13	0.08
10	0.6	0.54	0.49	0.33	0.28	0.15	0.09

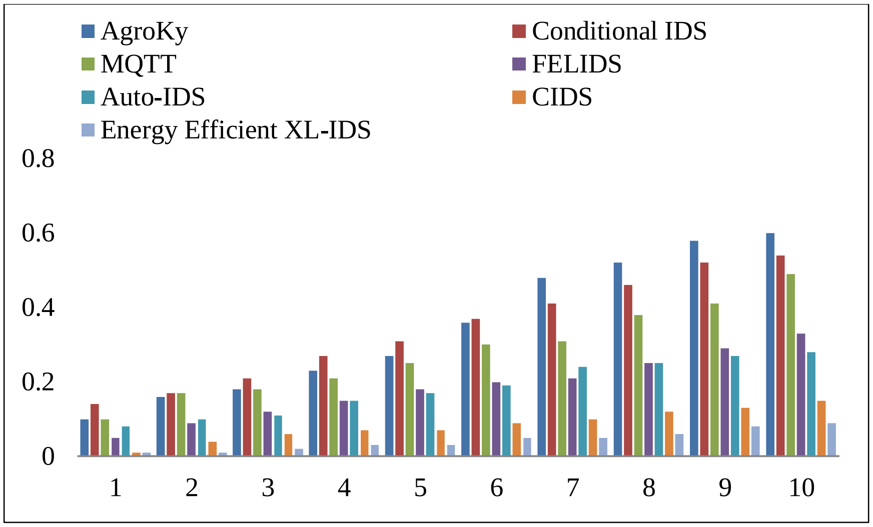


Fig. 9 Comparison of false positive rate

Table 4. Comparison of energy consumption models

Simulation Time	AgroKy	Conditional IDS	MQTT	FELIDS	Auto-IDS	CIDS	Energy Efficient XL-IDS (mJ)
100	1198.36	1199.96	1204.12	1226.39	1263.67	1279.72	1294.35
150	1184.26	1193.62	1201.36	1218.63	1216.56	1223.56	1235.24
200	1176.25	1184.63	1198.29	1216.28	1219.73	1228.72	1233.27
250	1161.14	1158.15	1187.98	1211.14	1214.65	1216.75	1204.64
300	1152.28	1147.97	1184.96	1208.38	1210.53	1235.63	1198.35
350	1149.37	1138.36	1176.98	1197.63	1199.61	1215.63	1198.24
400	1133.39	1121.97	1163.16	1186.42	1192.48	1198.26	1196.37
450	1121.98	1117.54	1158.11	1171.38	1175.43	1189.52	1195.46
500	1119.63	1116.63	1134.15	1163.11	1172.16	1186.26	1194.64

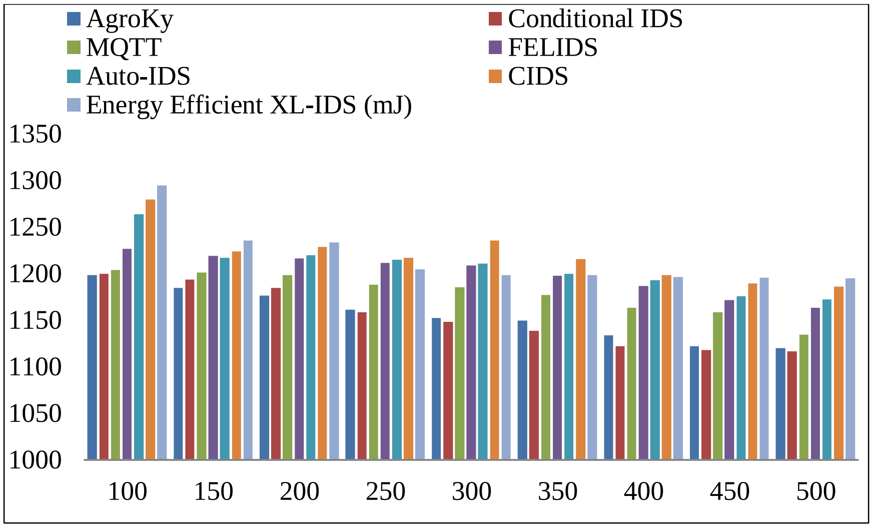


Fig. 10 Comparison of energy consumption in mJ

Hence, the strategy mentioned above has exhibited a greater lifespan through the effective utilization of energy to accomplish the data transfer process. Figure 11 illustrates the analysis of network lifetime by considering the number of nodes and the running time of the proposed model. By addressing energy consumption at various levels, our system minimizes redundant data transmissions and reduces the overall energy overhead associated with intrusion detection.

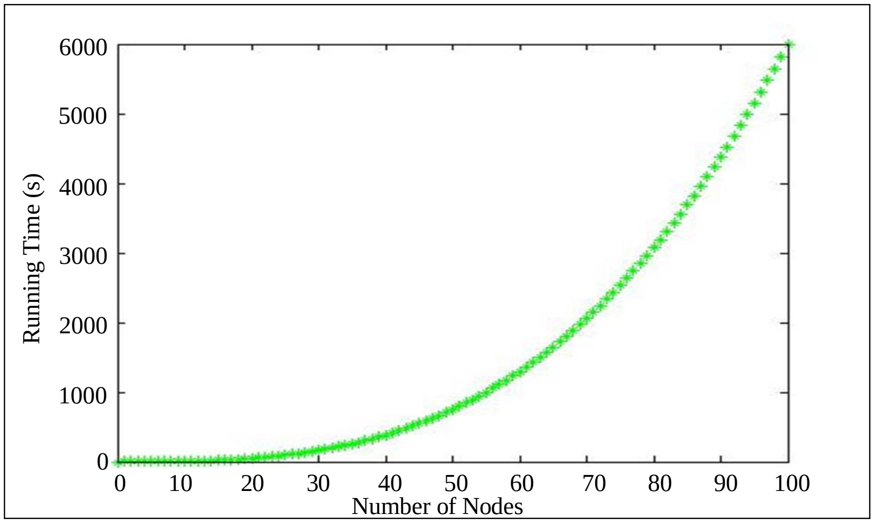


Fig. 11 Network lifetime of proposed model

5. Conclusion

Developing and implementing an Energy-Sensitive Clustering Algorithm within an XL-IDS model for agriculture atmosphere monitoring using WSN significantly enhances the efficiency, security, and sustainability of modern precision agriculture. This technology leverages the unique characteristics of WSNs and addresses the specific challenges posed by agriculture atmosphere monitoring. An energy-sensitive clustering algorithm for optimizing network performance and extending the operational lifetime of sensor nodes. Our algorithm considers the energy levels of individual nodes, their proximity to neighbors, and their suitability to serve as cluster heads. This approach ensures that cluster heads are selected judiciously, minimizing energy-intensive long-distance communication and facilitating efficient data aggregation.

Our model incorporates cross-layer intrusion detection mechanisms that operate at multiple protocol layers, thereby enhancing the accuracy of intrusion detection to 95.43 % while minimizing false positives and negatives. By analyzing data and events across these layers, our system can detect anomalies and intrusion patterns more effectively, safeguarding the integrity of collected data and the overall health of crops.

References

[1] Uferah Shafi et al., “Precision Agriculture Techniques and Practices: From Considerations to Applications,” *Sensors*, vol. 19, no. 17, pp. 1-25, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Divyansh Thakur et al., “Applicability of Wireless Sensor Networks in Precision Agriculture: A Review,” *Wireless Personal Communications*, vol. 107, pp. 471-512, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yemeserach Mekonnen et al., “Machine Learning Techniques in Wireless Sensor Network Based Precision Agriculture,” *Journal of the Electrochemical Society*, vol. 167, pp. 1-11, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] P. Sanjeevi et al., “Precision Agriculture and Farming Using Internet of Things Based on Wireless Sensor Network,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Laura García et al., “Deployment Strategies of Soil Monitoring WSN for Precision Agriculture Irrigation Scheduling in Rural Areas,” *Sensors*, vol. 21, no. 5, pp. 1-27, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Fekher Khelifi et al., “Monitoring System Based in Wireless Sensor Network for Precision Agriculture,” *Internet of Things (IoT)*, pp. 461-472, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Alexandros Zervopoulos et al., “Wireless Sensor Network Synchronization for Precision Agriculture Applications,” *Agriculture*, vol. 10, no. 3, pp. 1-20, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nisar Ahmad et al., “IOT Based Wireless Sensor Network for Precision Agriculture,” *2019 7th International Electrical Engineering Congress (iEECON)*, Hua Hin, Thailand, pp. 1-4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] D.D. Dasig, “Implementing IoT and Wireless Sensor Networks for Precision Agriculture,” *Internet of Things and Analytics for Agriculture*, vol. 2, pp. 23-44, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yousef E.M. Hamouda, and Mohammed M. Msallam, “Smart Heterogeneous Precision Agriculture Using Wireless Sensor Network Based on Extended Kalman Filter,” *Neural Computing and Applications*, vol. 31, pp. 5653-5669, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jerrin Simla A., Rekha Chakravarthy, and Megalan Leo L., "An Experimental Study of IoT-Based Topologies on MQTT Protocol for Agriculture Intrusion Detection," *Measurement: Sensors*, vol. 24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Abhishek Raghuvanshi et al., "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming," *Journal of Food Quality*, vol. 2022, pp. 1-8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Othmane Friha et al., "FELIDS: Federated Learning-Based Intrusion Detection System for Agricultural Internet of Things," *Journal of Parallel and Distributed Computing*, vol. 165, pp. 17-31, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Tanya Sood et al., "Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network," *Wireless Personal Communications*, vol. 126, pp. 911-931, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Geeta Singh, and Neelu Khare, "A Survey of Intrusion Detection from the Perspective of Intrusion Datasets and Machine Learning Techniques," *International Journal of Computers and Applications*, vol. 44, no. 7, pp. 659-669, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] G. Oussama et al., "Fast and Intelligent Irrigation System based on WSN," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yile Wang et al., "Image Detection System Based on Smart Sensor Network and Ecological Economy in the Context of Fine Agriculture," *Journal of Sensors*, vol. 2022, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Romany F. Mansour, "Blockchain Assisted Clustering with Intrusion Detection System for Industrial Internet of Things Environment," *Expert Systems with Applications*, vol. 207, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sakshi Anand, and Avinash Sharma, "AgroKy: An Approach for Enhancing Security Services in Precision Agriculture," *Measurement: Sensors*, vol. 24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdur Rehman Riaz et al., "Applying Adaptive Security Techniques for Risk Analysis of Internet of Things (IoT)-Based Smart Agriculture," *Sustainability*, vol. 14, no. 17, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Prince Rajak, Jaykumar Lachure, and Rajesh Doriya, "CNN-LSTM-Based IDS on Precision Farming for IIoT Data," *2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, Goa, India, pp. 99-103, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Muhammad Shoaib Farooq et al., "A Survey on the Role of IOT in Agriculture for the Implementation of Smart Livestock Environment," *IEEE Access*, vol. 10, pp. 9483-9505, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Nookala Venu, A. Arun Kumar, and A. Sanyasi Rao, "Smart Agriculture with Internet of Things and Unmanned Aerial Vehicles," *NeuroQuantology*, vol. 20, no. 6, pp. 9904-9914, 2022. [Google Scholar] [Publisher Link]

[24] Abhilash Singh et al., "AutoML-ID: Automated Machine Learning Model for Intrusion Detection Using Wireless Sensor Network," *Scientific Reports*, vol. 12, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Amira Zrelli, Cherfia Nakkach, and Tahar Ezzedine, "Cyber-Security for IoT Applications Based on ANN Algorithm," *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, Shenzhen, China, pp. 1-5, 2022. [CrossRef] [Google Scholar] [Publisher Link]