3-17-2023

A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming

Junaid Sajid
National University of Sciences and Technology

Kadhim Hayawi
Zayed University

Asad Waqar Malik
National University of Sciences and Technology

Zahid Anwar
North Dakota State University

Zouheir Trabelsi
United Arab Emirates University

applied sciences

MDPI

Article

A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming

Junaid Sajid [1], Kadhim Hayawi [2], Asad Waqar Malik [1,*], Zahid Anwar [3,*] and Zouheir Trabelsi [4]

[1] School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[2] College of Interdisciplinary Studies, Computational Systems, Zayed University, Abu Dhabi P.O. Box 144534, United Arab Emirates
[3] Department of Computer Science, The Sheila and Robert Challey Institute for Global Innovation and Growth, North Dakota State University, Fargo, ND 58105, USA
[4] College of Information Technology, United Arab Emirates University, Abu Dhabi P.O. Box 15551, United Arab Emirates
* Correspondence: asad.malik@seecs.edu.pk (A.W.M.); zahid.anwar@ndsu.edu (Z.A.)

Abstract: Precision agriculture and smart farming have received significant attention due to the advancements made in remote sensing technology to support agricultural efficiency. In large-scale agriculture, the role of unmanned aerial vehicles (UAVs) has increased in remote monitoring and collecting farm data at regular intervals. However, due to an open environment, UAVs can be hacked to malfunction and report false data. Due to limited battery life and flight times requiring frequent recharging, a compromised UAV wastes precious energy when performing unnecessary functions. Furthermore, it impacts other UAVs competing for charging times at the station, thus disrupting the entire data collection mechanism. In this paper, a fog computing-based smart farming framework is proposed that utilizes UAVs to gather data from IoT sensors deployed in farms and offloads it at fog sites deployed at the network edge. The framework adopts the concept of a charging token, where upon completing a trip, UAVs receive tokens from the fog node. These tokens can later be redeemed to charge the UAVs for their subsequent trips. An intrusion detection system is deployed at the fog nodes that utilize machine learning models to classify UAV behavior as malicious or benign. In the case of malicious classification, the fog node reduces the tokens, resulting in the UAV not being able to charge fully for the duration of the trip. Thus, such UAVs are automatically eliminated from the UAV pool. The results show a 99.7% accuracy in detecting intrusions. Moreover, due to token-based elimination, the system is able to conserve energy. The evaluation of CPU and memory usage benchmarks indicates that the system is capable of efficiently collecting smart-farm data, even in the presence of attacks.

Keywords: precision agriculture; unmanned aerial vehicles; smart farming; intrusion detection; fog nodes

Citation: Sajid, J.; Hayawi, K.; Malik, A.W.; Anwar, Z.; Trabelsi, Z. A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming. *Appl. Sci.* **2023**, *13*, 3857. https://doi.org/10.3390/app13063857

Academic Editors: Romano Lottering, Kabir Peerbhay and Samuel Adelabu

Received: 1 February 2023
Revised: 7 March 2023
Accepted: 8 March 2023
Published: 17 March 2023

1. Introduction

With rapid advancements being made in remote sensing technology, the role of the Internet of Things (IoT) is playing a significant role in precision agriculture. Many techniques are being used to collect and analyze crop data to improve farm productivity and maximize revenue [1]. In most cases, agriculture information is generated with the help of deployed sensors, collected through UAVs. The role of UAVs in data gathering and field monitoring has increased. The affordability and simplicity of operating UAVs for precision agriculture are significant factors in their adoption [2].

In smart farming, wireless sensors are deployed to obtain field information to increase productivity and convenience [3]. Sensors are readily available at relatively low costs and can be used to develop applications to facilitate production management, crop security, irrigation control, and scheduling [4]. However, UAV integration with smart farming

creates new security challenges [5]. As UAVs navigate in an open environment, they are increasingly susceptible to attacks that can cause them to be misguided, disrupted, or even physically taken over. Due to the omnipresence of UAV technology, several issues with UAV networks need to be taken into account, including communication, data collection, data security, storage, and supervision [6]. In precision agriculture, several UAVs work together to tackle the task of large-scale data gathering [7]. Due to the wireless nature of devices, it is important to consider the security aspect of the entire system before deployment. In many cases, the deployed devices are interconnected through short-range communication and are also able to connect through the internet [8].

A consequence of this increased connectivity is that such platforms become susceptible to vulnerabilities associated with GPS spoofing, GPS jamming, radio frequency interference, malware infiltration, man-in-the-middle, denial of service [9], denial of sleep [10], message replay and data feed interception [11]. If successfully exploited, these vulnerabilities can cause these systems to become a target of cyberattacks, where an intruder can penetrate and take control of the UAVs, interrupt activities, or modify the data gathered [12]. Besides vulnerabilities in wireless connectivity, UAVs are also susceptible to physical attacks whereby the attacker is physically adjacent and uses the close proximity to take control of the devices [13].

In the context of UAV-assisted precision agriculture where UAVs assist in a variety of tasks across several farms as illustrated in Figure 1, such attacks can have devastating impact. This impact includes but is not limited to completely damaging cropland, flooding of farm fields, and malicious spraying of pesticides, which might result in a significant consumption of chemicals [14]. These threats are classified as agricultural terrorism.

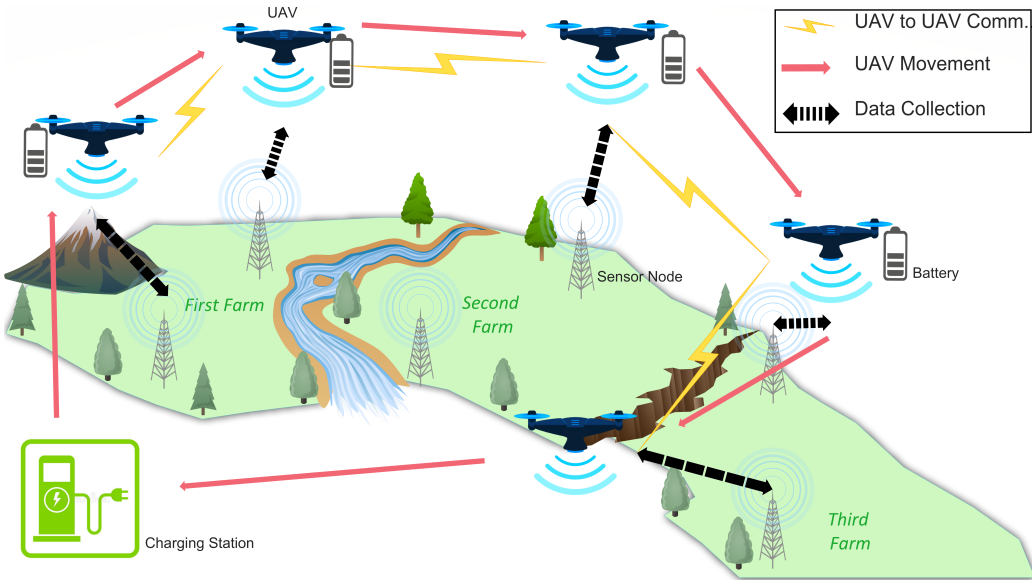

Figure 1. UAV-assisted precision agriculture scenario.

The Federal Bureau of Investigation (FBI) is alerting the agricultural sector that attackers may target farms more frequently during crucial planting and harvesting seasons and interrupt business activities, which would have a detrimental effect on the food supply chain. In a recently released alert, the FBI warned that ransomware attacks (https://www.beefmagazine.com/news/fbi-warns-cyberattacks-during-critical-ag-seasons, accessed on 14 December 2022) on six agricultural organizations during the autumn 2021 harvest and well as two strikes in early 2022 might affect the planting season due to the sabotage of seeds and fertilizer delivery. One of the largest meat processing companies, JBS, spent about USD 11 million in ransom to end a cyberattack last year (https://www.bbc.com/news/science-environment-61336659, accessed on 14 December 2022). A leading US agricultural company, AGCO, was the target of a ransomware attack in

May 2022 that majorly impacted their output. A consortium of authorized governmental cyber security experts from the United Kingdom, United States, and Australia issued a warning in April alerting that supply chains, a crucial component of the Western national infrastructure, might be targeted by state-sponsored Russian attackers.

The cybersecurity of technology that enables precision agriculture is a significant obstacle to its widespread adoption. To address this challenge, it is essential to develop a comprehensive framework that enhances the security of precision agriculture [15]. This research focuses on a subset of attacks that target the disruption of UAV data communication through techniques such as distributed denial-of-service (DDoS), unauthorized access, brute force, and infiltration. Compromised UAVs can significantly reduce the efficiency of the data collection system by reporting false data and consuming excessive energy for flight and hovering activities. They also compete for charge times on shared charging stations, thereby negatively impacting uncompromised UAVs.

This work proposes a smart farming framework that allows securing the use of UAVs for data collection through deployed sensors. Comprehensive models for sensors and UAV energy consumption and threat vectors have been developed. Furthermore, algorithms have been developed for farm data transmission and collection utilizing a fog computing architecture. A fog broker, a key central element that manages interactions between the UAVs and sensors, is utilized for deploying an intrusion detection system (IDS). The IDS that utilizes machine learning classification is developed to detect and flag compromised UAVs based on their behaviors. Flagged UAVs are then penalized through a coin-based system where the greater number of coins collected allows for a greater amount of charge. UAVs lose coins and ultimately charge proportionally to the degree of malicious behavior to minimize the level of disruption to the overall system.

The main contributions of the proposed work are listed as follows:

1. A novel toolkit was developed that supports UAV-based data collection mechanisms in smart farming. The data were collected from sensors deployed in the fields. A fog broker was used to manage all of the responsibilities and interactions of the UAVs, sensors, data transmission, and data collection.
2. A machine learning model was trained at the edge station based on the UAV-to-UAV communication logged and shared after every round. The trained model was then deployed to the UAVs and the model outcomes were shared with the fog node for identifying malicious behavior.
3. A coin-based recharge system was proposed to prune malicious UAVs. The UAV charging was based on the coins it received in lieu of the activities it performed, such as data transmission and recording during data gathering. UAVs exhibiting suspicious behaviors received fewer coins in that cycle. UAVs consistently exhibiting this behavior in multiple cycles were automatically removed from the system because of a lack of coins and, thereby, charge.
4. The innovation of this study lies in a framework that combines UAVs, IoT devices, and an IDS to enhance data collection in smart farming. Machine learning algorithms are used to detect and prevent attacks, and UAVs and IoT devices enable efficient and timely data collection. The IDS component addresses potential intrusion threats, and the XGBoost algorithm provides the best results for intrusion detection accuracy. The proposed framework has the potential to advance smart farming technology, benefiting the agriculture industry and society.

The rest of the article is organized as follows: Section 2 presents the related work. Section 3 covers the system model. The proposed methodology is presented in Section 4. The evaluations and results are given in Section 5, and the discussion and conclusion are provided in Sections 6 and 7, respectively.

2. Related Work

We are interested in related research that considers security issues in precision agriculture and smart farming assisted by UAVs. UAV performances can be negatively impacted

by malicious attacks because UAVs collect sensitive data that intruders may attempt to intercept in data transmission. Intrusion detection systems can help detect cyber attacks on UAVs and the data collected.

We found relatively limited research available in the use of machine learning techniques for intrusion detection in UAV-assisted precision agriculture. However, we did find related work in the general areas of smart farming, UAV-assisted smart farming, and intrusion detection systems that benefited our research. This section summarizes the latest research works in these areas and highlights the research gaps.

2.1. Smart Farming

Smart farming is described as a farming system in which innovative and cutting-edge technologies are used with conventional farming practices to increase farmland production quantity and quality while dramatically reducing manufacturing costs [16]. Smart farming and traditional farming are completely different from one another. Traditional farming practices include employing outdated equipment for labor and cultivating seasonal crops without first determining market demands and prices, or taking into account weather data from the weather service, among other things. Technological advances are used in smart farming, including smart devices, IoT sensors, cloud/fog computing, UAV data collection, and periodic assessments of various aspects. This makes farming simple and inexpensive with minimum labor costs. and results in improved crop yields and increased productivity [17]. The primary emphasis is on the integrated and coordinated implementation of new technologies into smart farms while offering sophisticated agriculture management that draws on collective expertise and judgment. Some noteworthy attempts include the Soil Scout [18] and Thoreau [19] projects, which monitor soil properties and farming conditions [20] using wireless sensor nodes.

While traditional farming devices are designed to have a strong connection and low power utilization, they are inadequate for carrying out sophisticated operations. IoT devices, in contrast, are linked and have the potential to offload operations to the cloud or spread them across several devices. The advantages of multiple farms linked with sensors and actuators connected across an IoT access point that deliver smart agricultural systems for end users are explored in [21]. The IoT devices are also linked to a server that keeps track of all the interconnected farms. IoT gateway-based surveillance software in [22] evaluates the leaf area index. Since the Internet of Things-based data analytics operates with a range of sensors, solutions can only accommodate homogeneous sensors.

Despite these efforts, a significant obstacle to widespread farmer adoption of such networked solutions remains, which is the availability of configurable hardware that can be programmed for customized data collection. A system employing open hardware to allow the creation of a smart farming framework is presented in [23] to address this difficulty. Furthermore, a proposed methodology in [24] introduces a smartphone-based smart agricultural system. Users of the system can operate the installed sensor modules or gather and evaluate agricultural data from the environment. The overlying infrastructure is adaptable and enables dispersed service deployment. These frameworks allow for the creation of reproducible IoT-based farming applications.

2.2. UAV-Assisted Smart Farming

Smart farming has become a reality with the growth of the IoT and unmanned aerial vehicles. IoT increases the value of gathered data through perceptual computation, automated data collection, and access by facilitating data flow between various sensors and other IoT devices. As a result, smart farms may employ productivity and managerial methods that are more timely and affordable [25]. Agricultural UAVs are notable practical developments in smart farming and are frequently employed by farmers [26,27] for regulating and supervising farming operations. Several UAVs are often intended to effectively pour water and various pesticides into territory where personal mobility is difficult and

the farms have varying altitudes. Recognizing the importance of this, the Massachusetts Institute of Technology designated UAVs as a green-tech tool for smart farming in 2014 [28].

Clusters of UAVs with diverse sensors and 3D cameras can cooperate with recent developments in swarm technologies, including mission-based administration, to provide farmers with a complete suite of soil management tools. UAVs designed for providing farming assistance are making it feasible for farmers to easily capture a bird's eye perspective of their fields in order to maintain and govern the farms properly. This dramatically lowers operating time, leading to greater steadiness in farm production, as well as precision. Various applications have helped several aspects of agriculture [26,28], including searching and applying fertilizer and pesticides, finding and eliminating weeds, sowing seeds, determining productivity and mapping out the land. Researchers have proposed a system [29] that utilizes UAV pictures to identify weeds prematurely in an Australian chili crop. The yield elevation of maize and sorghum crops in a farming field was also measured using UAV pictures [30]. Researchers have also [31] suggested a unique approach to taking UAV photos of farming fields and rebuilding three-dimensional images to observe the growth characteristics of the crops. UAVs are already being equipped with smart devices to conduct a variety of tasks in smart farming, including monitoring field conditions [32], collecting meteorological data, including temperature, humidity, wind speed, and air movement, among others [33], and improving crop yield [28].

In order to demonstrate real-time measurement impacting the amount and quality of grape yield, researchers have linked wireless sensor networks with a smart UAV system [34]. A UAV equipped with smart aerial sensors was created by Hernandez et al. [35] to record the grain volume within a trailer while forage is being harvested. Shamshiri et al. [36] have demonstrated the use of UAVs in solving a variety of challenges relating to palm oil plantation, including yield prediction, disease detection, and pest monitoring. Despite all of these UAV developments, numerous problems remain that must be addressed for improved deployment, including energy drain of UAVs, security hardening against cyber attacks, managing long communication distances, and carrying payloads [27,37]. For instance, since energy is a limited resource for UAVs, Islam et al. have concentrated on lowering energy usage in UAVs [38] but security against cyber attacks to prevent intrusion is still a critical challenge.

2.3. Intrusion Detection Systems

Network IDS: Machine learning-based approaches and, in particular, deep learning (DL) methods [39–42], are being used to produce cybersecurity solutions for securing communication for the Internet of Things and cyber-physical systems in the face of intrusions. To detect GPS spoofing, Manesh et al. [43] used supervised learning and artificial neural networks and Min et al. [44] developed a semi-supervised and unsupervised framework for intrusion detection. To increase the accuracy of classification, essential characteristics, including Doppler shift and SNRratio, have been chosen using feature engineering on the well-known KDD Cup 99 dataset and its variations [45,46]. To give an IDS improved generalization capabilities, Wang et al. [45] combined group convolution networks with snapshot ensemble learning. In another work, an IDS for UAV networks was created by Wang et al. [47] using the LSTM recurrent neural network. A further advanced strategy that combines XGBoost and DNN was proposed by Devan et al. [46]. While the deep neural network is used to create the classification, XGBoost is useful for extracting features and dimensionality reductions. A hybrid optimization-driven ensemble classification was created in [48] using a fog computing environment that combines multiple individual classifiers in order to improve overall prediction accuracy. A hybrid approach proposed in [49] combines association rule mining and classification methods to enhance the privacy and security levels of the network environment and improve the accuracy of intrusion detection. The aim of the study in [50] is to examine and assess intrusion detection systems designed for Agriculture 4.0 cybersecurity. The focus is on discussing the cybersecurity threats that these systems face and the metrics used to evaluate their performance.

UAV IDS: In critical situations, UAV systems are frequently utilized to communicate crucial data. The limits of the UAV infrastructure's computing and communication capacities, meanwhile, make them vulnerable to intrusions and attacks. Intrusion detection systems for UAVs or UAV IDS are often designed to recognize a variety of anomalies and vulnerability types, including malware such as ransomware, signals, route modification, tracking attacks, and GPS spoofing [51] in UAV systems. Bithas et al. [52] conducted a thorough study of machine learning algorithms for dealing with different UAV challenges, including channel modeling and resources [53], and employed LSTM and convolutional neural network techniques to create spatial–temporal deep learning on communication graphs. Abu et al. [41] studied an unsupervised learning-based technique to detect persistent spoofing in UAV interconnected networks. In contrasting to typical machine learning frameworks, the use of deep learning has greatly improved the detection accuracy for recently created intrusions that are challenging to identify using conventional machine learning methods [54]. Automated hyperparameter optimization (HPO) has grown in popularity in both research and commercial applications as a way to remove the impediments for average consumers [55]. Intrusion detection based on hyperparameter optimization has been previously investigated [56] and has shown to be very promising. The research in [57] discusses an agricultural information security framework that incorporates UAV technology and machine learning for data collection. The integration of these technologies promotes the development of the Internet and information security. The paper also proposes the use of a Double Deep Q-network algorithm to efficiently optimize the deployment of UAVs and a smart agricultural information management system for intrusion detection. We extended traditional hyperparameter optimization methods and used an advanced hyperparameter optimization technique for intrusion detection in this research.

2.4. Summary of Existing Literature

Based on a thorough examination of the literature, Table 1 compares the features of the most relevant research works to this proposed effort focusing on the mathematical modeling of smart farming systems as well as intrusion detection. It may be noted from the table that several studies address sensor-based smart farming frameworks, but most frameworks lack UAV integration to collect farming data. Similarly, there is limited research on intrusion detection in smart farming systems. The proposed framework is novel in that it combines aspects of smart farming, UAV based data collection, as well as proposes an advanced hyperparameter optimization-based intrusion detection system.

Table 1. Comparison of Related Work in Precision Agriculture and Intrusion Detection.

Authors	Env * S/R *	Int * Det *	M L *	Intg * Env *	Supported Application	UAV Data Collection	UAV Energy Model	U2U * Com *
W. H. Maes [4]	R	×	×	×	Remote Sensing	×	×	×
R. Mitchell [58]	S	✓	×	×	Behavior Specification	×	×	×
R. Dagar [17]	S	×	×	×	IoT in Agriculture	×	×	×
J. Doshi [20]	R	×	×	×	Monitoring	×	×	×
A. Raghuvanshi [59]	R	✓	✓	×	Risk Mitigation	×	×	×
A. W. Malik [60]	S	×	×	Fog	Farming Simulation Toolkit	✓	×	✓
M. Ryu [21]	R	×	×	×	Connected Farms	×	×	×

Table 1. *Cont.*

Authors	Env * S/R *	Int * Det *	M L *	Intg * Env *	Supported Application	UAV Data Collection	UAV Energy Model	U2U * Com *
J. Bauer [22]	R	×	×	×	Monitoring System	×	×	×
S. Trilles [23]	R	×	×	×	Vineyard Monitoring	×	×	×
N. Islam [29]	R	×	✓	×	Weed Detection	×	×	×
N. Chebrolu [31]	R	×	✓	×	Crop Monitoring	✓	×	×
D. Popescu [32]	R	×	×	×	Intelligent Monitoring	✓	×	×
N. islam [38]	S	×	×	×	Delay Aware	✓	×	×
X. Gao [40]	S	×	×	×	Intelligent Monitoring	✓	×	×
Q. Abu Al-Haija [41]	S	✓	✓	×	Classification System	×	×	✓
P. Devan [46]	S	✓	✓	×	Classification Model	×	×	×
B. Wang [47]	S	×	✓	×	Anomaly Detection	×	×	×
V. Kanimozhi [61]	S	✓	×	Cloud	Artificial Neural Network	×	×	×
R. kumar [62]	S	✓	✓	Fog	Smart Agriculture	✓	×	×
H. Rajadurai [63]	S	✓	✓	×	Stacked Ensemble Model	×	×	×
Proposed Work	S	✓	✓	Fog	Smart Farming	✓	✓	✓

* Env: Environment, S: Simulator, R: Real, Int: Intrusion, Det: Detection, ML: Machine Learning, Intg: Integrated, U2U: UAV to UAV, Com: Communication.

3. System Model

Consider an agricultural farm denoted as $\mathcal{F}$ having a width (w) and a length (l). The farms are sub-labeled as $f_1, f_2 \ldots f_m \in \mathcal{F}$, where m represents the total number of farms. There exist a total of n sensors $\mathcal{S}$ deployed to obtain field data. The framework can accommodate diversified sensors with different transmission times (T_s) and energy requirements (E_s). The sensor location is defined as S_{xy}. The sensors also serve as gateways, forwarding data across the farm in addition to generating their own data. The UAVs are used for data collection from sensors and offloading to the back-end server for further analysis and decision-making. Each UAV has an energy denoted as (E_u) and a communication range (R_u).

3.1. Ground Sensors Energy Model

It is assumed that $\mathcal{S}$ has two states namely active and passive. E_{sl} and E_{ac} are the energies consumed in the passive and active states, respectively. Therefore, the total energy consumed E_t is given in Equation (1) [64]:

$$E_t = E_{sl} + E_{ac} \tag{1}$$

$$E_{sl} = P_{sl} \times T_{sl} \tag{2}$$

Here, P_{sl} is the power usage, and T_{sl} is the amount of time spent in sleep mode. Likewise, the total energy used when in the active state E_{ac} is computed in Equation (3).

$$E_{ac} = E_m + E_d + E_p + E_t + E_r \tag{3}$$

In this case, E_m represents the energy consumed due to mode change, and E_d represents the energy consumed during data collection. E_p represents data processing energy and E_t and E_r represent the data transmitting and receiving energy, respectively.

3.2. UAVs Energy Consumption Model

The model supports two basic modes of operation for UAVs, i.e., flying and hovering. The power consumption in the flying mode is represented as P_η, and that consumed in the hover mode as P_ζ. Here, it is assumed that the UAV's flight paths are uniform, requiring no modification in terms of acceleration and deceleration. It is further assumed that rotary wing UAVs are used in this scenario, flying at a speed V. Thus, the energy consumption of the UAVs during flying, represented as E_η is defined as:

$$E_\eta = \frac{P_\eta}{V} \tag{4}$$

Here, the V is the speed of the UAV and is defined as:

$$P_\eta = P_1(1 + P_2V^2) + P_3\left(\sqrt{1 + \frac{V^4}{P_4^2}} - \frac{V^2}{P_4}\right)^{1/2} + P_5V^2 \tag{5}$$

where P_i , i = 1, ..., 5, are the parameters for the energy model specified in [65] and $P_1(1 + P_2V^2)$ is the blade profile power. $P_3\left(\sqrt{1 + \frac{V^4}{P_4^2}} - \frac{V^2}{P_4}\right)^{1/2}$ is the induced power, and P_5V^2 is the parasite power. The parasite power is the element needed to counter the parasite friction drag caused by the aircraft flying through the air, and the induced power is the element needed to counteract the induced drag produced during lift force to keep the aircraft in the air.

The power consumption for rotary-wing UAVs is provided by the finite value $P_1 + P_3$ for the exceptional case when the speed of the UAV is zero. Such power use is consistent with the rotary-wing UAV hovering in one place. However, if the UAV's flight speed is not zero, then parasite power emerges. While the induced power reduces with UAV speed V, both the blade profile power and the parasite power increase with UAV speed.

Hovering: The UAV interacts with each sensor only when it is hovering at one of the optimum hovering locations. The energy consumption when UAVs hover is represented by E_ζ and is defined as:

$$E_\zeta = (P_h + P_c)T_\zeta \tag{6}$$

where P_h is the power consumed in the hovering, P_c is the power consumed by the UAV communicating with the ground node and T_ζ is the time of hovering. These parameters are expressed in [65].

3.3. UAV Data Collection

Notably, data are gathered from the deployed sensor by a number of N UAVs. It is considered that the UAVs and deployed sensors communicate via uplink-based orthogonal frequency division multiple access (OFDMA). K continuous links are supported by the UAVs for data collection. Additionally, we provide a distributed system where UAVs share data with surrounding fog sites. Since the inserted sensors may be portable, there may be sporadic communication between the sensors and UAVs with significant packet loss.

Therefore, the line of sight (LoS) must be maintained for communication to be successful. The LoS probability is calculated as in [64].

$$p_{LoS} = \frac{1}{1 + o \times exp(\gamma[\psi - \nu])} \tag{7}$$

where ψ is the elevation angle between the sensor S_{xy} and the UAV U_{xy}, and o and γ are constants and are determined by the communication frequency and range. The probability increases with increasing UAV height; therefore, deployed sensors may only be allocated to the j_{th} UAV if the chance of LoS is near to 1. Consequently, the condition of the connection between the sensor and the UAV is:

$$d_{ij} = \frac{a_j}{sin(p_{LoS})} \tag{8}$$

where d_{ij} is the distance between the i_{th} ground node and the j_{th} UAV and a_j is the height of the UAV from the ground node.

Considering there are a × b sensors spread out over the farm, the coverage time t_{cov} of the UAV is calculated as:

$$t_{cov} = \Sigma_a \Sigma_b T_{ab} + \frac{2}{N} \Sigma_i \Sigma_j S_{ij} \tag{9}$$

where T_{ab} is the time required for the UAVs to travel from one ground node to the other node, and N is the total number of UAVs that were utilized to collect the data.

We employed a set of brokers B to control the fog sites to analyze the collected data. A fog broker was in charge of the effective use of fog services near the target consumers. The broker distributed the resources to other brokers on the site. This supported latency-sensitive IoT applications by reducing the communication time. $N_d = d_m + d_n$, where d_m is the network delay between the sensors and UAVs, and d_n is the network delay between the UAV and the designated fog site and is dependent upon the distance between ground nodes. The network cost C, on the other hand, is a linear function of distance and is given as:

$$C = \vartheta \left(d_{m,n} + \Sigma_{k \in B \& n \neq o} d_{n,o} \right) \tag{10}$$

where ϑ is constant, $d_{m,n}$ is the distance between the m_{th} UAV and its local broker n and $d_{n,o}$ is the distance of the local broker renting the computation resource $n \in B$.

3.4. Threat Model

In order to detect cyberattacks, the proposed intrusion detection system is explained in Section 4.4.2 and the attacker goals and capabilities are detailed here. The attacker's primary goal is to hamper the data collection process so that the farmer has an erroneous or inaccurate picture of the state of the farm. An example of this is that the UAVs report readings that cause the system to indicate that soil moisture is sufficient, while in reality it is dry. To accomplish this, the attacker locates UAVs, gains access to the control system, and tampers with the data communication. Compromised UAVs end up flying over the farmland needlessly consuming energy, providing incorrect data to the fog broker, and stealing valuable charging time from other legitimate UAVs at the charging station. The attacker achieves these goals by executing one or more of the following attacks:

- **Distributed denial of service attack** : In a DDoS attack, the attacker attempts to hamper the UAV's data collection process by sending a large number of messages to needlessly engage the UAV in processing useless packets. As a result, either the UAV is unable to communicate with neighboring UAVs or it suffers delays in UAV-to-UAV and UAV-to-sensor communication. Such attacks consume UAV energy significantly.
- **Heart bleed** : In this attack, the attacker attempts to gain unauthorized access to the UAVs by scanning the UAV-to-UAV communication to identify vulnerabilities. For scanning, the attacker can use specialized devices installed nearby; moreover, the

UAVs can also be used for initiating the scans. After compromising a UAV, the attacker injects malware and fake data into other connected UAVs; thus, trying to disrupt the data collection process.

- **Brute force** : In this attack, the attacker attempts to gain unauthorized access to the fog portal through UAVs. It is assumed that the admin portal is accessible by UAVs through a wireless link after providing the appropriate credentials. This interface is normally used by the administrator from the fog node to connect to multiple UAVs and update software, configure data collection routes, and perform other administrative tasks. After compromising a UAV the attacker injects malware and fake data into other connected UAVs; thus, trying to disrupt the data collection process.
- **Infiltration attack** : The goal of the infiltration attack is to compromise the UAV network and gain control over the UAVs themselves. Once access is achieved, the UAVs allow for passive reconnaissance, allowing the attacker to gather information about the network and its devices. This information can be used to plan further attacks by identifying and exploiting vulnerabilities that can be used for privilege escalation.

The CICIDS2017 dataset [66] closely reflects actual real-world data on the following attacks: brute force FTP, brute force SSH, dos, ddos, heart bleed, web attacks, infiltration attacks, and botnets. Here, the observations pertinent to ddos, heart bleed, brute force, and infiltration attacks are used. Additionally, this dataset contains network traffic evaluation performed through CIC FlowMeter, which involved processes labeled according to the timestamp, source, and destination IP addresses, source, and destination port numbers, protocol, and attacks. The dataset is split into training and testing. The training models are deployed on UAVs in a simulation framework to efficiently identify the attacks. Further, the dataset is integrated into the simulation framework in the form of an attack module so that as the simulation progresses the data collected by the UAVs is affected and the proposed intrusion detection system attempts to detect this behavior and weed out the compromised UAVs.

4. Methodology

The proposed system consists of farms, unmanned aerial vehicles, deployed sensors, fog brokers, and fog nodes, as shown in Figure 2. The framework allows the simulation of large-scale farms with sensors deployed to monitor the farms, and UAVs are used to gather information periodically. The information is offloaded at the connected fog node through the fog broker. Moreover, the system detects malicious UAV behavior through a machine-learning model deployed at the UAVs. The main modules are elaborated on below.

4.1. Smart Farms

The framework allows the user to define farms, deploy sensors and configure the data collection process through UAVs. Here, we assumed that the farms are large-scale and comprise flat and mountainous terrain. Therefore, due to the uneven terrain, ground-to-ground communication is not a suitable option [67]. Therefore, data collection through UAVs are more suitable for uneven farming lands.

4.2. Broker

The broker functionality is shown in Figure 3. A broker is a static node placed near a fog site to manage the site's fog resources as well as control management aspects of the UAVs such as their scheduling. The broker node also collaborates with other brokers for UAV sharing. Each fog node owns a few UAVs but to cover the large-scale area, they may need additional resources from nearby fog sites. Therefore, a collaborative broker-based design is proposed. The broker can lease resources from neighboring fog sides which are later settled through a bartering mechanism. The brokers maintain a history of the resources leased and allocated.

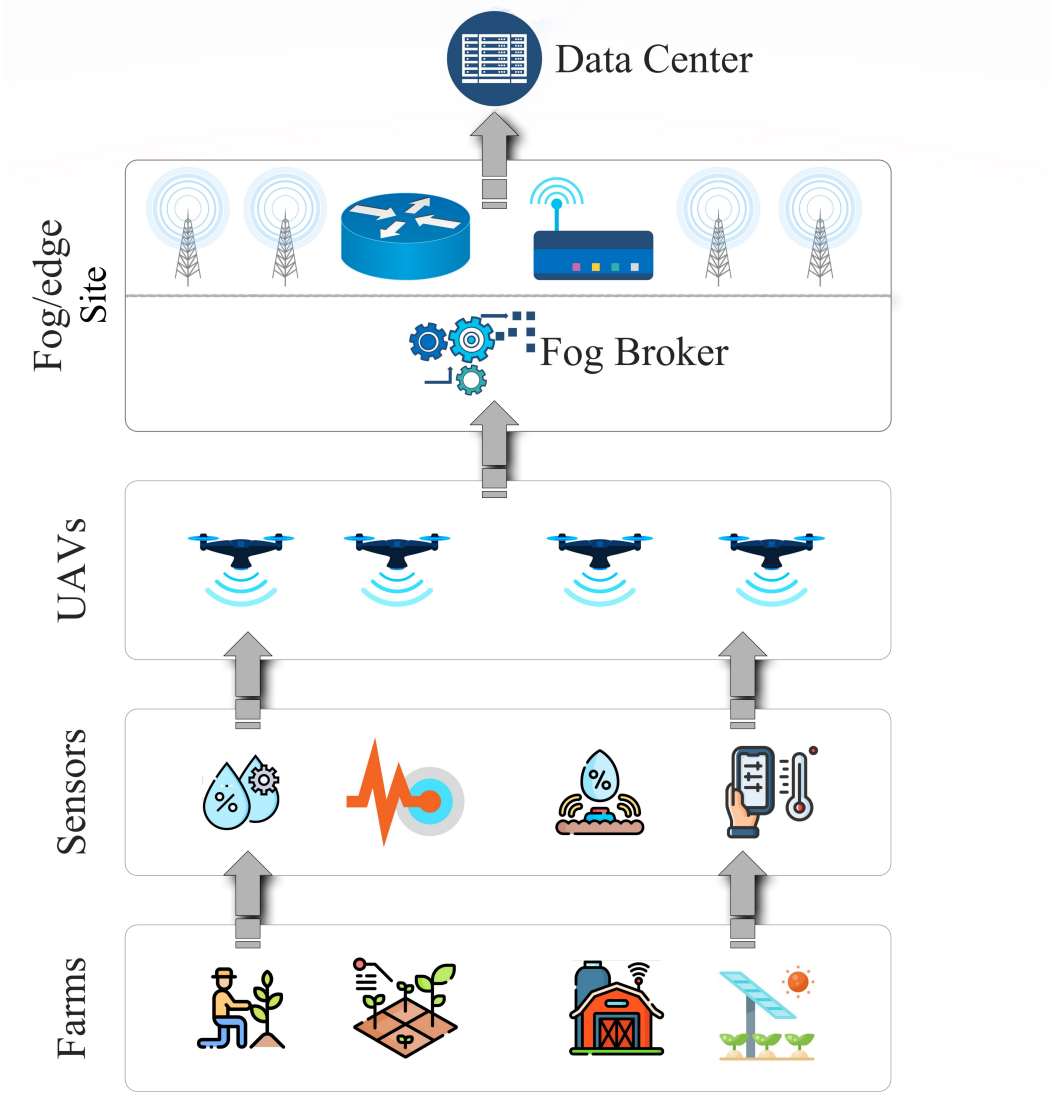

Figure 2. Fog-based layered architecture.

4.3. Sensors

The proposed framework facilitates the deployment of both stationary and mobile sensors to collect data to increase agricultural production. The transmission, storage, and battery life of the sensors vary and the framework provisions the behavioral simulation of heterogeneous sensors. Additionally, the sensors facilitate the ad hoc method of information transmission to nearby gateway nodes. The architecture of a typical sensor node is shown in Figure 3. In the proposed work, UAVs serve as mobile gateway nodes to collect data from both fixed and mobile sensors. In the traditional case of a deployed wireless sensor network, the data are sent to a cluster head of the gateway node. Furthermore, such methods consume a great deal of energy in the leader selection and route-finding processes. Therefore, a mobile gateway is employed to collect the data through UAVs and maximize the usage of sensors and lengthen their lifetime.

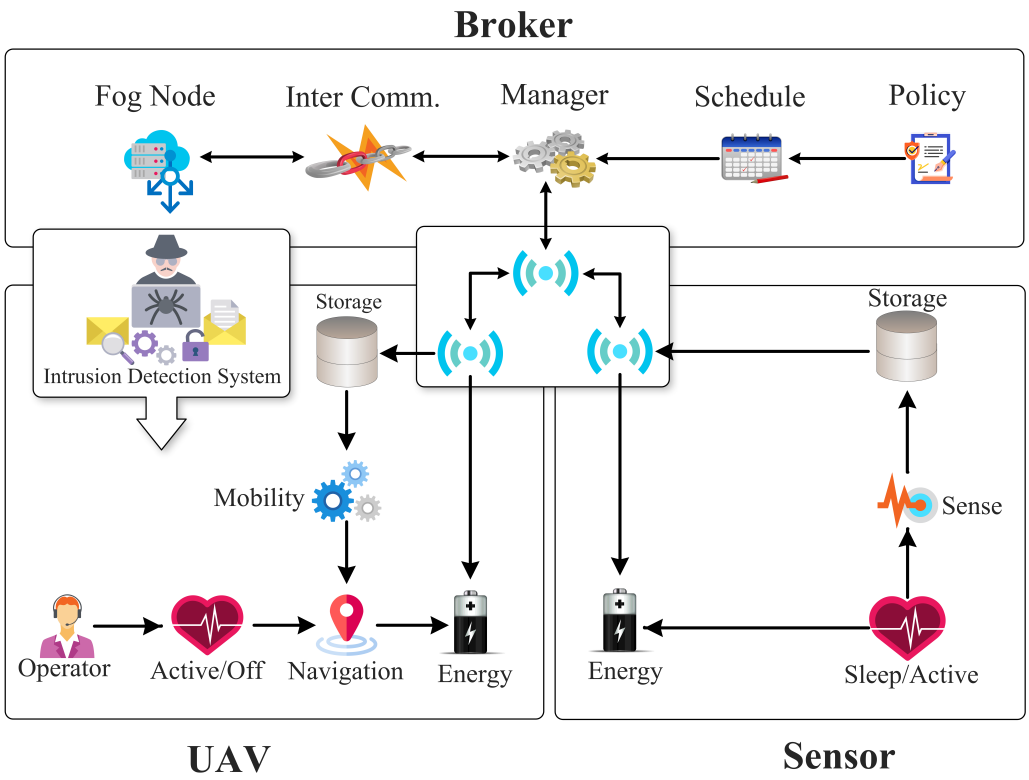

Figure 3. Detailed Architecture Diagram of Proposed Framework.

4.4. Unmanned Ariel Vehicles (UAVs)

The data collection process is executed with the help of unmanned aerial vehicles, which collect data from the sensors deployed at the fog site. The path of the UAVs is pre-configured. A fleet of UAVs flies through this pre-defined path to collect the data. On cycle completion, UAVs return to the charging station to recharge their batteries for the next trip.

4.4.1. UAV Behavior-Based Charging

A major limitation of UAV-assisted data collection is effectively managing UAVs' rapidly depleting energy banks during operation. Therefore, in the proposed work, we have integrated this aspect into the UAV behavior. The only way for the UAV to acquire a charge is by transmitting data and recording transactions at the fog node. The algorithm for UAV Charging is provided in Algorithm 1. The UAVs are allowed to use the charging spot only when they have the desired coin which they acquire by completing transactions with the fog node. The number of charging coins in this framework is assumed to be an integer for simplicity. The forwarding and recording costs for a single message are referred to as c_f and c_r, respectively. The forwarding and recording of messages is a prerequisite for obtaining coins to participate in the charging process. The charging coin (P_c) is assigned based on the following equation.

$$P_c = \begin{cases} if c_r == c_f & c_r/c_f \\ if c_r > c_f & c_f/c_r \\ if c_f > c_r & c_r/c_f \end{cases} \tag{11}$$

Algorithm 1 UAVCharging

```
UAV: list of UAVs
U.Coin: reward value
U.E: reward value
U.P: Path
U.CList: Received coin list
S: list of deployed sensors
procedure UAVDATACOLLECTION
    while true do
        U_i ← MoveOnPath(U.P)                          ▷ Moving UAVs on predefined paths
        if U_i is Connected to S_j then                ▷ comm range with S_j
            U_i.data ← S_j                             ▷ get data from sensor
        end if
        U_i.Communicate(UAV)                           ▷ Send msgs to UAVs in swarm
        U_i.Rec(msg from U_k)                          ▷ Comm msgs from other UAVs
        B ← U_i.ModelTest(msg)                         ▷ identify abnormal behavior
        if B is NORMAL then                            ▷ Normal behavior
            U_i.send(U.Coin, 1)                        ▷ send complete coin value
        else
            U_i.send(U.Coin, 0.5)                      ▷ Otherwise reduce coin value
        end if
        U_i.CList = Rec(C from UAV)                    ▷ Collect coin values
        U_i.Coin = Accumulate(U_i.CList)
        if U_i path Completed then
            U_i.Upload(B)                              ▷ upload data to broker
            U_i.E ← Recharge(U_i.Coin)                 ▷ get recharge on coins value
        end if
    end while
end procedure
```

In the above equation, the UAV's record and forward attributes are used to generate the charging coin. In case the UAV recollect matches with the forwarding parameter, one complete charging coin is issued. However, on any malicious behavior, the charging coin value is determined based on the ratio of collection and forwarding. In other words, a UAV is allowed to acquire a charge using the coin before the next trip. The flight route of each UAV is already available with the broker node which helps determine the energy needed to complete the trip. Therefore, if the UAV is unable to obtain the complete energy for the next trip, the broker tags it as malicious requiring a log inspection. Apart from the energy-based elimination from the UAV pool, the malicious activity is also monitored in the UAV network, which is explained in the next section.

4.4.2. UAV-to-UAV Based Intrusion Detection Mechanism

During data collection, the UAVs communicate with each other and exchange trajectory information along with other parameters, such as residual energy. This information is shared periodically, assuming that UAVs have sufficient energy to bear the communication cost. The UAVs move in the form of a fleet; where each UAV is covering a different path but is connected with other UAVs through a wireless connection. The entire UAV communication is logged for subsequent use in model training.

The proposed intrusion detection model is trained on the collected data at the fog broker and deployed at UAVs and attempts to identify these attacks. The proposed architecture consists of multiple stages, i.e., data prepossessing, feature engineering, and intrusion detection. First, a dataset is gathered to evaluate the performance of the system. A *k*-means-based cluster sampling technique is used to create a highly representative subset of the data while preventing class imbalance. The dataset is treated throughout the feature engineering process to eliminate redundant and unnecessary features using information gain-based and correlation-based feature selection approaches, and the kernel principal component analysis model is used to further decrease the dimensions and noisy features.

It is suggested that a hyperparameter-based optimization IDS be used to effectively identify both known and unidentified intrusions as discussed in [56]. The system is composed of several tiers, where the first tier consists of four tree-based machine learners namely decision tree, random forest, extra tree, and extreme gradient boost, which are used

to identify known attacks. By integrating the output of the four base learners from the first tier and optimizing the learners, the second tier uses a stacking ensemble model and the Bayesian optimization-tree-structured Parzen estimator approach to further increase the intrusion detection accuracy. An anomaly-based intrusion detection system is built in the next stage to identify unknown attacks. The cluster-labeling *k*-means model is used as the 3rd tier of the intrusion detection system to successfully differentiate attack data from regular samples. The Bayesian optimization-Gaussian process technique and two biased classifiers make up the fourth tier of the IDS, which is utilized to improve the model and decrease classification errors in the *CL-k*-means. Each test sample's detection outcome is ultimately reported, and it may be a known attack with a type, an unidentified attack, or typical benign traffic.

5. Evaluation

The proposed framework is evaluated for measuring the effectiveness of the hyperparameter optimization-based intrusion detection as well as the efficiency of the algorithm executing on the UAVs.

5.1. Machine Learning Framework

For the effectiveness study, the proposed methodology is evaluated in terms of accuracy, precision, recall, F1 score, root mean square error, and R-squared score as evaluation metrics. The generated dataset is provided to the intrusion detection system that utilizes XGBoost random forest (RF), decision tree (DT), extra tree (ET), stacking, and *k*-means algorithms. The detailed results of the intrusion detection effectiveness evaluation are given in Figure 4. It can be seen that all algorithms perform well due to hyperparameter optimization with XGBoost showing the best results with 99.77% accuracy, 0.1055 root mean square error, and 99.81% R-Squared score. These results indicate that algorithms perform well and fit the data model. Further, XGBoost can handle large datasets. Therefore, performing classification or regression using XGBoost typically begins with an estimate, determines the similarities value, and obtains a tree for each potential threshold [68].

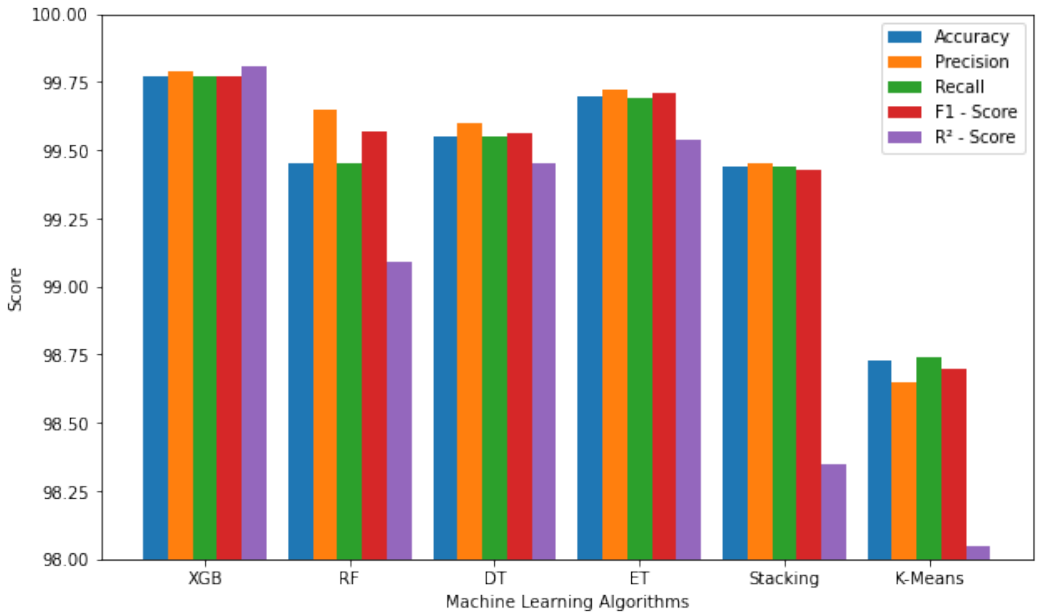

Figure 4. Effectiveness of the Intrusion detection system using the selected machine learning algorithms.

A comparison of the effectiveness with respect to related works is shown in Table 2. The proposed model has improved accuracy, precision, recall, and F1 score as compared to other state-of-the-art related works.

Table 2. Comparison with other models.

Method	Accuracy	Precision	Recall	F1 Score	Time in Sec
STDG [53]	99.13	98.60	98.70	0.986	1848
SU-IDS [44]	99.13	99.65	98.60	0.991	15,243
DPMH [69]	98.95	95.82	95.81	0.958	-
DC [70]	98.55	98.22	99.59	0.983	34,986
PCA-RF [71]	99.60	99.60	99	0.996	-
Proposed	**99.77**	**99.79**	**99.771**	**0.997**	**772**

5.2. Simulation Framework

The proposed UAV-assisted data collection framework is evaluated using a simulation model developed in AnyLogic (www.anylogic.com, accessed on 15 December 2022)—a multi-method simulation software that allows the integration of multiple modeling paradigms including discrete event, agent-based, and system dynamics modeling. The simulation model is designed to represent the behavior of the UAVs, fog nodes, and broker nodes, as well as their interactions in the data collection process. The simulation model includes several components including the fog sites, brokers, sensors and UAVs, the parameters for which are provided in Table 3. The UAVs are modeled as autonomous agents that can move around in a 2D space, collect data from different locations, and transmit data to the nearest fog node. The fog nodes are modeled as stationary nodes that receive UAV data and store them temporarily before transmitting them to the broker node. The broker node collects data from the fog nodes, processes them, and stores them in a database.

Table 3. Simulation and System Specifications.

Parameters	Values
Fog Sites	3–6
Fog Brokers	3–6
Sensors	Up to 600
UAVs	5–15
CPU	3.60 GHz Inter Core i7-6700K
RAM	8 GB
OS	Windows 10 Pro
Simulator	AnyLogic

The simulation model is parameterized with realistic values based on existing literature and real-world data. The energy consumption of the UAVs is modeled based on the type of UAV, speed and the distance traveled, while the transmission range of the UAVs and the fog nodes is modeled based on the signal strength and interference in the environment. The charging rate of the UAVs is also modeled based on the transaction costs and the amount of data transmitted. The simulation model is used to evaluate the performance of the proposed framework under different scenarios and conditions. The impact of the number of UAVs and fog nodes, the data collection rate, and the charging rate on the overall performance of the system is evaluated. The simulation model is also used to evaluate the robustness of the system under different types of attacks, such as denial of service attacks, spoofing attacks, and jamming attacks.

The simulation results are analyzed and compared to existing literature to validate the effectiveness of the proposed framework. The simulation results show that the proposed framework can achieve higher data collection rates and better energy efficiency compared to existing methods. The simulation results also show that the proposed framework is robust against various types of attacks, demonstrating the effectiveness of the proposed intrusion detection system.

In our proposed framework, we used the CICIDS2017 dataset to evaluate the performance of our UAV-assisted intrusion detection system. CICIDS2017 is a publicly available dataset for evaluating intrusion detection systems. It is a labeled dataset with various types of network traffic, including normal traffic and several types of attacks. The dataset contains a total of 80 features, including flow duration, protocol, source, and destination IP addresses, source and destination port numbers, and packet and byte counts. Some of the features are calculated from the network flow, such as the flow duration, packet count, and byte count, while others are extracted from the packet header, such as the protocol and port numbers. We used the flow duration, protocol, and packet count parameters from the dataset to train and test our machine learning models. We also used the source and destination IP addresses and port numbers to identify the type of attack.

The AnyLogic simulator was used to generate synthetic network traffic data for testing our intrusion detection system. The simulator also allowed us to visualize the behavior of the system and test different scenarios to evaluate the performance.

UAV energy consumption: Conserving energy is one of the critical challenges for UAV-based systems. In the proposed UAV model, the energy is consumed when a UAV moves, communicates, collects data, and hovers. The energy consumption in terms of speed is shown in Figure 5 and can be seen to be relatively high when the speed of the UAV is either too high or too low. The figure shows the energy consumption of three subsets of the energy, i.e., parasite, induced power, and blade profile. The figure illustrates that approximately 14 m/s is the ideal speed for achieving the most efficient energy consumption.

In the proposed work, the broker initiates the data collection process on multiple routes; therefore, Figure 6, shows the UAV residual energy with simulation time. Each route has a variable length causing UAVs to take different times to complete the task. The first path is the longest as it covers more area to collect data from deployed sensors; thus, UAVs consumed more energy to collect the data. The third path is the shortest because of the small coverage area of the fog site where the UAVs consumed less energy. In the first route, UAVs took more time and consumed around 80% of their energy. In the case of a benign scenario, the UAVs have full charge after every cycle. On the second route, it takes around 60% of the residual energy and takes relatively less time to complete the path. The same is the case with the third route. In case of malicious behavior, the UAV acquires a lower charge after every trip and is eventually removed from the group. Moreover, the deployed model detects the malicious behavior using the energy and communication parameters; thus, helping to send the UAV for inspection before offloading the data at the fog node. Figure 7 shows the residual energy when UAVs become malicious with simulation time. It is assumed that a UAV is 80% malicious because it participates in only 20% of the required recording and transmission. In this case, the UAV will only have 20% more charging. In the first route, the UAV does not have enough charging to complete its route and eventually is removed from the system. Similarly, in the second and third routes, malicious UAVs are automatically removed from the system after completing two rounds due to zero charging.

Resource utilization—the proposed framework is benchmarked in terms of resource usage, i.e., memory and CPU. These resources are used effectively by a well-constructed system. The memory consumption is shown in Figure 8 with varying nodes, i.e., UAVs/sensors. UAVs, brokers, farms, and sensors that have been deployed are included in this list of nodes. With 200 UAVs, only 4.5% of memory is utilized, whereas with 400 UAVs, 6.4% of memory is used. When the number of UAVs increases to 600, only 9.1% of memory is occupied, indicating a linear increase in memory usage with the number of UAVs. Notably, no memory leaks are noticed during the simulation run. The CPU consumption is shown in Figure 9. CPU usage escalates as the number of sensors increases. In this scenario, with 200 UAVs, 30% of CPU is used, whereas with 400 UAVs, 35% of CPU is utilized. When the number of UAVs increases to 600, the CPU usage reaches 39% only, which includes, computational algorithms, mobility models, energy modules, and communication links between the UAVs, installed sensors, brokers, and fog sites.

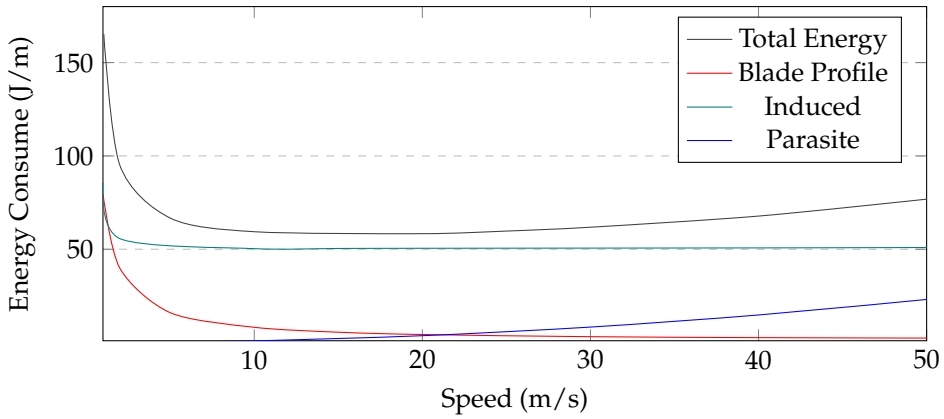

Figure 5. UAV's Consumed Energy with Respect to Speed.

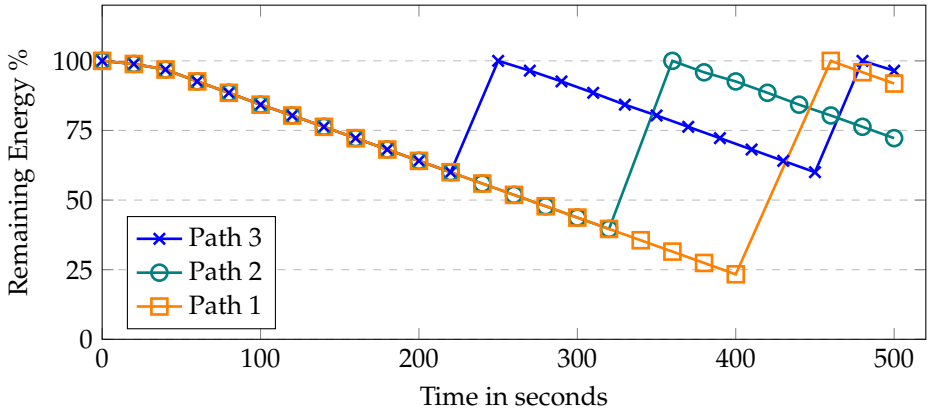

Figure 6. UAV's residual energy with respect to time.

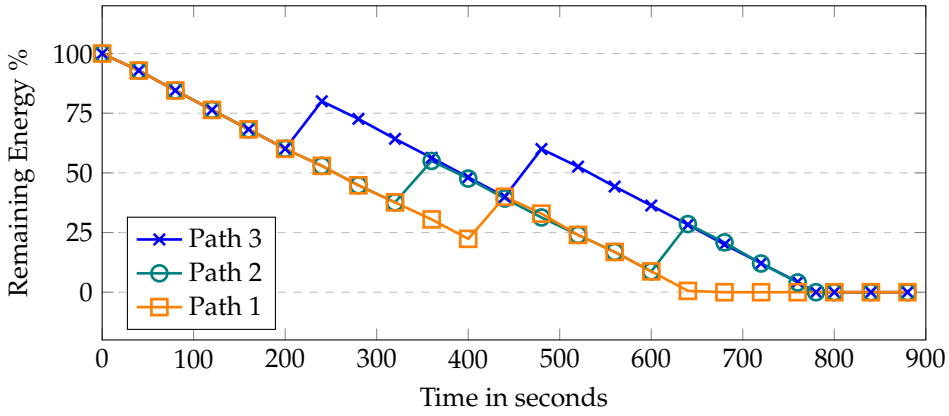

Figure 7. UAV's remaining energy when the UAV becomes malicious with respect to time.

UAV2UAV communication delay—the communication delay between UAVs is seen in Figure 10. The average delay is calculated by increasing the number of deployed sensors and different UAVs. Here, the UAVs gathered information from the sensors. According to availability, either the nearby sensor or the remote sensor communicates with the UAV for the transmission of the data. However, it has been noted that as the number of UAVs increases, the communication delay between the UAVs also increases.

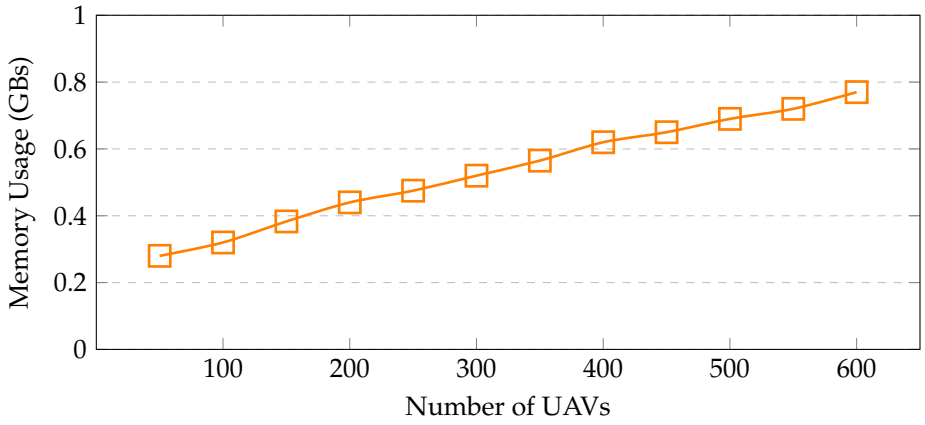

Figure 8. Memory utilization with increasing sensors.

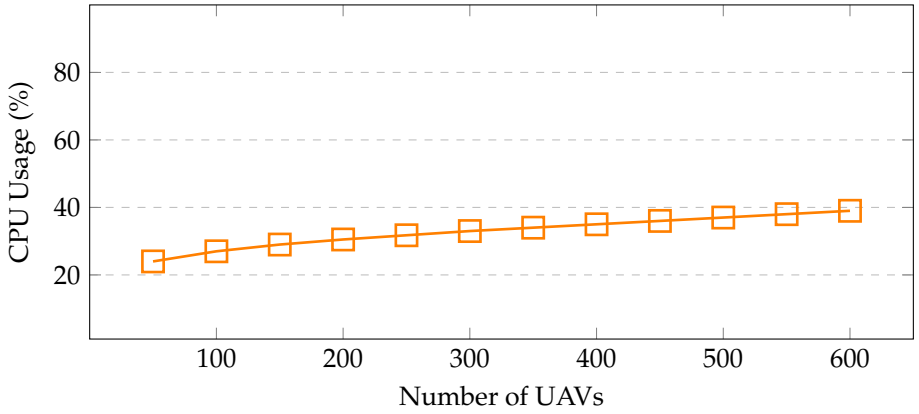

Figure 9. CPU Utilization with Increasing UAVs.

Transmission delay—the amount of time needed to send or receive a packet is called the transmission time or delay. When a UAV communicates with the sensor, it takes some time to receive the packets. The typical communication delay among UAVs and deployed sensors is seen in Figure 11. It is important to note that the delay grows as more sensors are placed. Due to the overlapping transmission ranges, several sensors attempt to interact with the UAVs, which causes increased channel congestion.

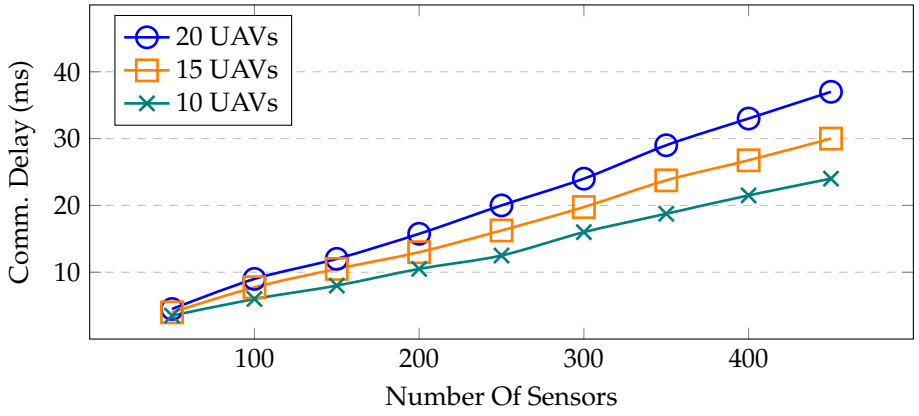

Figure 10. Average UAV-to-UAV communication delay with different numbers of sensors and UAVs.

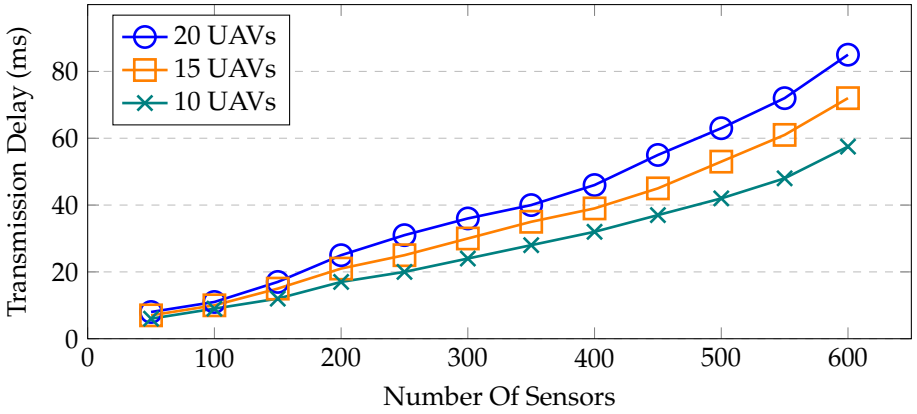

Figure 11. Transmission delay between sensors and UAVs.

6. Discussion

The results clearly indicate the increased security and the data-collection efficiency of the UAV-assisted smart farming framework that utilizes energy constraints and an intrusion detection system. The UAVs have a limited battery and are only allowed to charge by transmitting data and recording transactions at the fog node. This approach incentivizes the UAVs to identify malicious activities that may result in excluding the UAVs from the trusted network.

The proposed work is evaluated with various machine learning models as well as the other network parameters. In most of the existing works, authors are only focused on utilizing limited features for the machine learning model; thus, overlooking critical parameters such as UAV energy, transmission delay, and the impact of cyber-attacks on UAV's energy. This work presents an extensive framework that covers the data collection, sensors integrated environment, and role of fog nodes for recharging the UAVs.

The CPU and memory are the important parameters to gauge the scalability of devices inside the framework. With the increased number of UAVs, a linear relation is observed in terms of CPU and memory usage. The utilization of resources reported with 600 UAVs in a simulation framework require only 9.1% memory, and corresponding CPU utilization is 39%. Further, we observed that the speed of UAVs has a direct impact on their energy and in order to cover large-scale areas, a 14 m/s speed needs to be maintained for maximum utilization of UAVs. Moreover, amongst the machine learning models, adopted, XGBoost showed the best performance with 99.77% accuracy.

7. Conclusions

In recent years, smart farming technology has rapidly advanced and has significantly contributed to the improvement of crop yields. To further improve the efficiency of data collection in smart farming, this research proposes a framework that utilizes unmanned aerial vehicles (UAVs) and Internet of Things (IoT) devices. However, this open environment is vulnerable to intrusions, which can hinder the data collection process and ultimately reduce agricultural productivity. To address this potential threat, the research proposes an intrusion detection system (IDS) integrated into a fog-based UAV-IoT farm data collection system. The IDS utilizes machine learning algorithms that are trained on the CICIDS2017 dataset, which is publicly available, to detect and prevent intrusions. A layer-based intrusion detection approach is considered to detect both known and zero-day attacks. For known attacks, a signature-based IDS is used and uses XGBoost, extra tree, random forest, and decision tree algorithms. For zero-day attacks, clustering techniques are used, which include the K-means algorithm. The evaluation results show that XGBoost provides the best results, as it can detect intrusions with 99.77% accuracy, with an F1 score of 0.1055 RMSE and a 99.81% R-squared score. The modular design is developed to implement and benchmark the proposed work in terms of UAV energy, transmission, and communication delays. The proposed IDS integrated with the fog-based UAV-IoT farm data collection

system can improve the security and efficiency of smart farming, which can ultimately lead to increased crop yield and improved agricultural productivity. In the future, the research will aim to improve the intrusion detection system using machine vision and extensive deep learning techniques.

Author Contributions: Conceptualization, J.S., Z.A. and A.W.M.; methodology, Z.A. and A.W.M..; software, J.S. and A.W.M; validation, A.W.M; formal analysis, Z.A.; investigation, J.S., K.H, A.W.M. and Z.A.; resources, Z.A. and Z.T.; data curation, J.S., A.W.M. and Z.A.; writing original draft preparation, J.S., K.H., A.W.M, Z.A. and Z.T.; writing review and editing, A.W.M and Z.A.; visualization, J.S, A.W.M. and Z.A.; supervision, K.H., A.W.M., Z.A. and Z.T.; project administration, K.H., A.W.M., Z.A. and Z.T.; funding acquisition, K.H., Z.A. and Z.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Sheila and Robert Challey Institute for Global Innovation & Growth at North Dakota State University, USA, and Zayed University under the Cluster Research Grant R20140, UAE.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data may be requested by reaching out to authors through email.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kiani, F.; Seyyedabbasi, A. Wireless sensor network and Internet of Things in precision agriculture. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9* . [CrossRef]
2. Maddikunta, P.K.R.; Hakak, S.; Alazab, M.; Bhattacharya, S.; Gadekallu, T.R.; Khan, W.Z.; Pham, Q.V. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE Sens. J.* **2021**, *21*, 17608–17619. [CrossRef]
3. Mendez, G.R.; Yunus, M.A.M.; Mukhopadhyay, S.C. A WiFi based smart wireless sensor network for monitoring an agricultural environment. In Proceedings of the 2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings, Graz, Austria, 13–16 May 2012; IEEE: New York, NY, USA, 2012; pp. 2640–2645.
4. Maes, W.H.; Steppe, K. Perspectives for remote sensing with unmanned aerial vehicles in precision agriculture. *Trends Plant Sci.* **2019**, *24*, 152–164. [CrossRef]
5. Nguyen, M.T.; Nguyen, C.V.; Do, H.T.; Hua, H.T.; Tran, T.A.; Nguyen, A.D.; Ala, G.; Viola, F. Uav-assisted data collection in wireless sensor networks: A comprehensive survey. *Electronics* **2021**, *10*, 2603. [CrossRef]
6. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [CrossRef]
7. Ju, C.; Son, H.I. Multiple UAV systems for agricultural applications: Control, implementation, and evaluation. *Electronics* **2018**, *7*, 162. [CrossRef]
8. Faraci, G.; Grasso, C.; Schembra, G. Fog in the clouds: UAVs to provide edge computing to IoT devices. *ACM Trans. Internet Technol. (TOIT)* **2020**, *20*, 1–26. [CrossRef]
9. Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 1–20. [CrossRef]
10. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
11. Krishna, C.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; IEEE: New York, NY, USA, 2017; pp. 194–199.
12. Challita, U.; Ferdowsi, A.; Chen, M.; Saad, W. Machine learning for wireless connectivity and security of cellular-connected UAVs. *IEEE Wirel. Commun.* **2019**, *26*, 28–35. [CrossRef]
13. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4112. [CrossRef]
14. Bodkhe, U.; Tanwar, S.; Bhattacharya, P.; Kumar, N. Blockchain for precision irrigation: Opportunities and challenges. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e4059. [CrossRef]
15. Delavarpour, N.; Koparan, C.; Nowatzki, J.; Bajwa, S.; Sun, X. A technical study on UAV characteristics for precision agriculture applications and associated practical challenges. *Remote Sens.* **2021**, *13*, 1204. [CrossRef]
16. Panchasara, H.; Samrat, N.H.; Islam, N. Greenhouse gas emissions trends and mitigation measures in Australian agriculture sector—A review. *Agriculture* **2021**, *11*, 85. [CrossRef]

17. Dagar, R.; Som, S.; Khatri, S.K. Smart farming–IoT in agriculture. In Proceedings of the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018; IEEE: New York, NY, USA, 2018; pp. 1052–1056.
18. Tiusanen, M.J. Soil scouts: Description and performance of single hop wireless underground sensor nodes. *Ad Hoc Netw.* **2013**, *11*, 1610–1618. [CrossRef]
19. Zhang, X.; Andreyev, A.; Zumpf, C.; Negri, M.C.; Guha, S.; Ghosh, M. Thoreau: A subterranean wireless sensing network for agriculture and the environment. In Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, 1–4 May 2017; IEEE: New York, NY, USA, 2017; pp. 78–84.
20. Doshi, J.; Patel, T.; kumar Bharti, S. Smart Farming using IoT, a solution for optimally monitoring farming conditions. *Procedia Comput. Sci.* **2019**, *160*, 746–751. [CrossRef]
21. Ryu, M.; Yun, J.; Miao, T.; Ahn, I.Y.; Choi, S.C.; Kim, J. Design and implementation of a connected farm for smart farming system. In Proceedings of the 2015 IEEE SENSORS, Busan, Republic of Korea, 1–4 November 2015; IEEE: New York, NY, USA, 2015; pp. 1–4.
22. Bauer, J.; Aschenbruck, N. Design and implementation of an agricultural monitoring system for smart farming. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
23. Trilles, S.; González-Pérez, A.; Huerta, J. A comprehensive IoT node proposal using open hardware. A smart farming use case to monitor vineyards. *Electronics* **2018**, *7*, 419. [CrossRef]
24. Xue-Fen, W.; Yi, Y.; Tao, Z.; Jing-Wen, Z.; Sardar, M.S. Design of distributed agricultural service node with smartphone in-field access supporting for smart farming in Beijing-Tianjin-Hebei region. *Sens. Mater.* **2018**, *30*, 2281–2293. [CrossRef]
25. Glaroudis, D.; Iossifides, A.; Chatzimisios, P. Survey, comparison and research challenges of IoT application protocols for smart farming. *Comput. Netw.* **2020**, *168*, 107037. [CrossRef]
26. Sharma, R. Review on Application of Drone Systems in Precision Agriculture. *J. Adv. Res. Electron. Eng. Technol.* **2021**, *7*, 5–7.
27. Muchiri, G.; Kimathi, S. A review of applications and potential applications of UAV. In Proceedings of the Sustainable Research and Innovation Conference, April 4, 2022 ; pp. 280–283.
28. Boursianis, A.D.; Papadopoulou, M.S.; Diamantoulakis, P.; Liopa-Tsakalidi, A.; Barouchas, P.; Salahas, G.; Karagiannidis, G.; Wan, S.; Goudos, S.K. Internet of Things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review. *Internet Things* **2022**, *18*, 100187. [CrossRef]
29. Islam, N.; Rashid, M.M.; Wibowo, S.; Wasimi, S.; Morshed, A.; Xu, C.; Moore, S. Machine learning based approach for Weed Detection in Chilli field using RGB images. In Proceedings of the International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Fuzhou, China, 30 July–1 August 2020; Springer: New York, NY, USA, 2020; pp. 1097–1105.
30. Malambo, L.; Popescu, S.C.; Murray, S.C.; Putman, E.; Pugh, N.A.; Horne, D.W.; Richardson, G.; Sheridan, R.; Rooney, W.L.; Avant, R.; et al. Multitemporal field-based plant height estimation using 3D point clouds generated from small unmanned aerial systems high-resolution imagery. *Int. J. Appl. Earth Obs. Geoinf.* **2018**, *64*, 31–42. [CrossRef]
31. Chebrolu, N.; Läbe, T.; Stachniss, C. Robust long-term registration of UAV images of crop fields for precision agriculture. *IEEE Robot. Autom. Lett.* **2018**, *3*, 3097–3104. [CrossRef]
32. Popescu, D.; Stoican, F.; Stamatescu, G.; Ichim, L.; Dragana, C. Advanced UAV–WSN system for intelligent monitoring in precision agriculture. *Sensors* **2020**, *20*, 817. [CrossRef] [PubMed]
33. Raja, L.; Vyas, S. The study of technological development in the field of smart farming. In *Smart Farming Technologies for Sustainable Agricultural Development*; IGI Global: Hershey, PA, USA, 2019; pp. 1–24.
34. Spachos, P.; Gregori, S. Integration of wireless sensor networks and smart uavs for precision viticulture. *IEEE Internet Comput.* **2019**, *23*, 8–16. [CrossRef]
35. Hernandez, A.; Murcia, H.; Copot, C.; De Keyser, R. Towards the development of a smart flying sensor: Illustration in the field of precision agriculture. *Sensors* **2015**, *15*, 16688–16709. [CrossRef]
36. Shamshiri, R.R.; Hameed, I.A.; Balasundram, S.K.; Ahmad, D.; Weltzien, C.; Yamin, M. Fundamental research on unmanned aerial vehicles to support precision agriculture in oil palm plantations. In *Agricultural Robots-Fundamentals and Application*; Intechopen, 2018 ; pp. 91–116.
37. Von Bueren, S.K.; Burkart, A.; Hueni, A.; Rascher, U.; Tuohy, M.P.; Yule, I.J. Deploying four optical UAV-based sensors over grassland: Challenges and limitations. *Biogeosciences* **2015**, *12*, 163–175. [CrossRef]
38. Islam, N.; Sithamparanathan, K.; Chavez, K.G.; Scott, J.; Eltom, H. Energy efficient and delay aware ternary-state transceivers for aerial base stations. *Digit. Commun. Netw.* **2019**, *5*, 40–50. [CrossRef]
39. Choudhary, G.; Sharma, V.; You, I.; Yim, K.; Chen, R.; Cho, J.H. Intrusion detection systems for networked unmanned aerial vehicles: A survey. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–28 June 2018; IEEE: New York, NY, USA, 2018; pp. 560–565.
40. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access* **2019**, *7*, 82512–82521. [CrossRef]
41. Abu Al-Haija, Q.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. *Electronics* **2020**, *9*, 2152. [CrossRef]

42. Abu Al-Haija, Q.; Al Badawi, A. High-performance intrusion detection system for networked UAVs via deep learning. *Neural Comput. Appl.* **2022**, *34*, 10885–10900. [CrossRef]
43. Manesh, M.R.; Kenney, J.; Hu, W.C.; Devabhaktuni, V.K.; Kaabouch, N. Detection of GPS spoofing attacks on unmanned aerial systems. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Vegas, NV, USA, 11–14 January 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
44. Min, E.; Long, J.; Liu, Q.; Cui, J.; Cai, Z.; Ma, J. Su-ids: A semi-supervised and unsupervised framework for network intrusion detection. In Proceedings of the International Conference on Cloud Computing and Security, Haikou, China, 8–10 June 2018; Springer: New York, NY, USA, 2018; pp. 322–334.
45. Wang, A.; Wang, W.; Zhou, H.; Zhang, J. Network intrusion detection algorithm combined with group convolution network and snapshot ensemble. *Symmetry* **2021**, *13*, 1814. [CrossRef]
46. Devan, P.; Khare, N. An efficient XGBoost–DNN-based classification model for network intrusion detection system. *Neural Comput. Appl.* **2020**, *32*, 12499–12514. [CrossRef]
47. Wang, B.; Wang, Z.; Liu, L.; Liu, D.; Peng, X. Data-driven anomaly detection for UAV sensor data based on deep learning prediction model. In Proceedings of the 2019 Prognostics and System Health Management Conference (PHM-Paris), Paris, France, 2–5 May 2019; IEEE: New York, NY, USA, 2019; pp. 286–290.
48. MP, R.; Daniya, T.; Mano Paul, P.; Rajakumar, S. Intrusion detection using optimized ensemble classification in fog computing paradigm. *Knowl.-Based Syst.* **2022**, *252*, 109364.
49. Safara, F.; Souri, A.; Serrizadeh, M. Improved intrusion detection method for communication networks using association rule mining and artificial neural networks. *IET Commun.* **2020**, *14*, 1192–1197. [CrossRef]
50. Ferrag, M.A.; Shu, L.; Friha, O.; Yang, X. Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA J. Autom. Sin.* **2021**, *9*, 407–436. [CrossRef]
51. Zhao, L.; Alipour-Fanid, A.; Slawski, M.; Zeng, K. Prediction-time efficient classification using feature computational dependencies. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, UK, 19–23 August 2018; pp. 2787–2796.
52. Bithas, P.S.; Michailidis, E.T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A.G. A survey on machine-learning techniques for UAV-based communications. *Sensors* **2019**, *19*, 5170. [CrossRef] [PubMed]
53. Yao, Y.; Su, L.; Lu, Z.; Liu, B. Stdeepgraph: Spatial-temporal deep learning on communication graphs for long-term network attack detection. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security And Privacy in Computing And Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; IEEE: New York, NY, USA, 2019; pp. 120–127.
54. Chowdhury, M.M.U.; Hammond, F.; Konowicz, G.; Xin, C.; Wu, H.; Li, J. A few-shot deep learning approach for improved intrusion detection. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; IEEE: New York, NY, USA, 2017; pp. 456–462.
55. Yu, T.; Zhu, H. Hyper-parameter optimization: A review of algorithms and applications. *arXiv* **2020**, arXiv:2003.05689.
56. Kunang, Y.N.; Nurmaini, S.; Stiawan, D.; Suprapto, B.Y. Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *J. Inf. Secur. Appl.* **2021**, *58*, 102804. [CrossRef]
57. Fu, R.; Ren, X.; Li, Y.; Wu, Y.; Sun, H.; Al-Absi, M.A. Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet Things J.* **2023**. [CrossRef]
58. Mitchell, R.; Chen, R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Trans. Syst. Man, Cybern. Syst.* **2013**, *44*, 593–604. [CrossRef]
59. Raghuvanshi, A.; Singh, U.K.; Sajja, G.S.; Pallathadka, H.; Asenso, E.; Kamal, M.; Singh, A.; Phasinam, K. Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming. *J. Food Qual.* **2022**, *2022*, 3955514. [CrossRef]
60. Malik, A.W.; Rahman, A.U.; Qayyum, T.; Ravana, S.D. Leveraging fog computing for sustainable smart farming using distributed simulation. *IEEE Internet Things J.* **2020**, *7*, 3300–3309. [CrossRef]
61. Kanimozhi, V.; Jacob, T.P. Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 4–6 April 2019; IEEE: New York, NY, USA, 2019; pp. 0033–0036.
62. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Gadekallu, T.R.; Srivastava, G. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Comput. Netw.* **2021**, *187*, 107819. [CrossRef]
63. Rajadurai, H.; Gandhi, U.D. A stacked ensemble learning model for intrusion detection in wireless network. *Neural Comput. Appl.* **2020**, *34*, 15387–15395. [CrossRef]
64. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Mobile Internet of Things: Can UAVs provide an energy-efficient mobile architecture? In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; IEEE: New York, NY, USA, 2016; pp. 1–6.
65. Zeng, Y.; Xu, J.; Zhang, R. Energy minimization for wireless communication with rotary-wing UAV. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2329–2345. [CrossRef]

66. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp* **2018**, *1*, 108–116.
67. Olasupo, T.O. Propagation modeling of IoT devices for deployment in multi-level hilly urban environments. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; IEEE: New York, NY, USA, 2018; pp. 346–352.
68. Mitchell, R.; Adinets, A.; Rao, T.; Frank, E. Xgboost: Scalable GPU accelerated learning. *arXiv* **2018**, arXiv:1806.11248
69. Elmasry, W.; Akbulut, A.; Zaim, A.H. Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Comput. Netw.* **2020**, *168*, 107042. [CrossRef]
70. Vijayanand, R.; Devaraj, D.; Kannapiran, B. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Comput. Secur.* **2018**, *77*, 304–314. [CrossRef]
71. Abdulhammed, R.; Faezipour, M.; Musafer, H.; Abuzneid, A. Efficient network intrusion detection using pca-based dimensionality reduction of features. In Proceedings of the 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 18–20 June 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.