applied sciences

MDPI

Article

Preliminary Examination of Emergent Threat and Risk Landscapes in Intelligent Harvesting Robots

Nabil Moukafih [1,*], Gregory Epiphaniou [1], Carsten Maple [1], Chris Chavasse [2] and John Moran [2]

[1] WMG, University of Warwick, Coventry CV4 7AL, UK
[2] Muddy Machines Ltd., London SW6 4SL, UK
* Correspondence: nabil.moukafih@warwick.ac.uk

Abstract: Recently, many farmers have started using robots to help with labour-intensive harvesting operations and deal with labour shortage that was also a negative consequence of the recent COVID-19 pandemic. Intelligent harvesting robots make farming more efficient and productive. However, and like any other technology, intelligent harvesting robots come with a security risk, as threats can damage the robotic system and wreak havoc before the farmer/operator realizes it. This paper focuses on analysing the threats against the security of harvesting robots alongside with the safety implications that may rise if the robotic system is compromised. We analysed an actual asparagus harvesting robot and looked at others in the literature. We identified several security threats which we classified into five categories: network, hardware, software, Artificial Intelligence (AI) and cloud security issues. We selected three interesting attack scenarios for a deeper analysis. Our results suggest that these robots have a large attack surface that can lead to exploits with immense financial and operational impacts.

Keywords: intelligent harvesting; robotics; security assessment; AI; intelligent farming

Citation: Moukafih, N.; Epiphaniou, G.; Maple, C.; Chavasse, C.; Moran, J. Preliminary Examination of Emergent Threat and Risk Landscapes in Intelligent Harvesting Robots. *Appl. Sci.* **2022**, *12*, 12931. https://doi.org/10.3390/app122412931

Received: 11 October 2022
Accepted: 9 December 2022
Published: 16 December 2022

1. Introduction

In the last few years, there has been a growing effort to deploy robots in our environment to perform our daily tasks. From assistance and entertainment robots used in homes [1], to those working in assembly lines in industry [2] and all the way to those deployed in military [3] and professional facilities. For industrial applications, data show that the operational stock of industrial robots has tripled over the past decade, with more than three million robots in use across various industries [4]. In agriculture, robots are used due to their efficient and increased performance in reducing manpower and resource consumption [5]. This is interesting as worker shortage became a significant issue with COVID-19: travel restrictions, lock-downs and soaring wage costs pushed many farmers to turn to machines as an alternative, as is the case in Italian vineyards [6].

This increased reliance on agricultural robots in the post-COVID-19 era comes with security implications that need to be considered. On one hand, while there has been a decent effort in the research community to assess security in robotics [7,8], data show that there is still work to be conducted in this area. A recently published technical report about adversarial activity per section in 2021 [9] shows that most security researchers focus on assessing vulnerabilities in websites (96%), APIs (50%) and android (29%) amongst other technologies. On the other hand, existing research only looks at security in robotics on a general setting deployed in a general environment. While this will certainly lead to identifying threats, the complexity and impact of each threat varies from one environment to another. In other words, the same vector will have a significantly different impact if the targeted robot is used to carry out teleoperated surgical operations compared to another used for manufacturing [10]. Finally, research in intelligent farming tends to focus more on physical threats, IoT threats and, more generally, threats against information

and communication technologies without considering the presence of intelligent robots in this ecosystem [11]. This paper examines the security threats to intelligent harvesting robots while considering all the key components involved in this operation. It presents the following main findings:

- an overview of the key components of intelligent harvest architecture and an in-depth analysis of safety and security challenges;
- presentation of potential adversarial scenarios as use cases that link between system vulnerabilities, AI-specific vulnerabilities and hardware challenges in intelligent harvesting robots;
- an assessment of the potential impact of the identified use cases from an operational and financial perspective.

The remainder of this paper is structured as follows: Section 2 examines the related work of the security and safety issues of robots in other fields. In Section 3, we present the architecture of intelligent harvesting robots with the key components. In Section 4, we present the identified security and safety threats in robots used in intelligent harvesting. Finally, we conclude the paper in Section 6.

2. Related Work

Security and safety has always been an important factor to consider when using robots in any field. The aim of security is to protect the assets and services in the robotic environment from disruption, theft, or exploitation by unauthorized users. Safety on the other hand focuses on protecting the workeres around the robots, particularly employees who interact with a robot during programming, maintenance, testing, setup or adjustment. It is important to note that while employee safety is the main concern, robots are just as much a danger to a business's bottom line as they are to workers. Although in research, there has been much more interest in safety than security to reduce incidents that can lead to serious injury or even devastating results such as loss of human lives, many researchers have begun to investigate more incidents caused by malicious attacks as they represent a very challenging issue [12,13]. Hacking and controlling robots usually result in serious economic and financial losses, but the impact depends on the task at hand and the environment in which the robot operates.

In medical fields for example, some attacks can evade robot security controls to cause unexpected and sudden robot behaviors. This is dangerous for robots used to perform surgery, as it can cause patient injury, robot damage, or system unavailability in the middle of the surgery [14]. Although safety measurements are important for all types of robots, the problems and solutions are different. For example, safety in industrial robots is acheived via keeping humans out of the robot's workspace. However for surgical robots, the surgical team enter the workspace and physically interact with the robot that is also attached to the anesthetized patient [15]. This difference in the environment can also contribute to early detection by only focusing on certain physical features and the behaviour of the robot [16].

In another robot application, attacks on home-based robots can have a significant impact on user privacy and safety. Attackers can use hacked robot's cameras and microphones to spy on family members [17]. The link between home-based robots and voice-based assistants such as Alexa or Siri further widens attack surface, as the latter also poses security and privacy concerns [18]. If the robot can talk or allow an attacker to talk through its speaker, it could tell voice-based assistants to unlock doors and disable home alarms to allow burglars free access, which also raises a safety concern.

Industrial robots are generally larger, more powerful and have a precise movement. Due to these characteristics, attacks against industrial robots can have more dangerous scenarios with direct safety implications [19]. The authors in [20] highlighted four main threat scenarios that have impact on the accuracy, integrity and safety requirements of industrial robots. Moreover, the financial impact is on a large scale. Building industrial robots is more expensive and the loss will be more drastic if the number of compromised

robots is high. Disruption of production due the unavailability of robots will also lead to huge financial losses.

Note that all research in security of intelligent agriculture tends to focus more on physical threats such as weather conditions and climate change [21] and threats against IoT and heavy machinery connected online [11]. Other researchers focused on robotic security deployed in general setting [22], but no work has been conducted on the security and safety of intelligent harvesting robots. The authors in [23] claims that threats against robotics, IA and IoT can lead to disaster in crop harvesting which would lead to food shortage. In this work, we examined an actual robot for harvesting asparagus. As a result, we managed to identify safety and security issues of agricultural robots used for intelligent harvesting. The document begins by analyzing the environment in which the intelligent harvesting robot operates, then identifies and analyzes the security threats. Table summarizes the related work discussed in this section.

Table 1 summarizes the related work discussed in this section.

Table 1. Summary of related work.

Reference	Description
[12]	Highlights bot security threats, including communication and software. The authors claimed that there was not enough effort to prepare cyber-safe robots.
[13]	The authors performed a security vulnerability analysis of programmable robotic systems written in java and python and reported the main security findings. The work indicates that traditional access control systems cannot detect recent vulnerabilities or defend against the latest evolving cybersecurity and physical attacks on the availability, integrity and confidentiality of robotic systems.
[14]	The proposed work demonstrated cyber-physical attacks on the control system of surgical robots in the event when the attacker is able to install a malware to strategically inject faults into the control system at critical junctures during surgery. The results suggest that successful attacks can cause sudden jumps and unpredicted behaviours on surgical robots.
[15]	The paper proposes a safety design approach for computer-assisted surgery systems after performing a risk assessment to identify potential hazards. At the end, the authors proposed safety strategies to follow to prevent injury even in the event of component failures of computer-assisted surgery systems.
[16]	This paper investigates how a cyber-attack on a rescue robot can adversely affect its operation and impair an emergency response operation. They launched several attacks and analysed the behaviour of the rescue robot. Results suggest that using physical indicators can contribute to early detection and decision making.
[17]	Authors analysed the cyber security problems in modern robots. To do this, they applied a risk assessment and threat modelling methodology on robots from multiple vendors. Results state that there are several security and privacy issues that have consequences in many areas of applications such as home, military, health and industry.
[18]	The authors proposed a comprehensive systemic security assessment of voice-based assistant in used robots used in homes. The work considers several factors in the design of the technology that widens the attack surface. The authors also discussed some countermeasure to the identified threats and presented some open questions that still further research.

Table 1. *Cont.*

Reference	Description
[19]	This chapter summarises approaches to the coordinated assurance of safety and security of collaborative industrial robots. The work specifically focuses on human-robot interaction and collaboration in manufacturing from a security perspective. The use-case focus a robot named COBOT in which the performed threat modelling and risk assessment to identify and prioritise threats. The identified challenges are not limited only to technical factors, they only considered socio-technical factors.
[20]	Focusing on industrial robots as use case, this work provides a holistic view of the security issues that arise in designing and securely deploying controlled manufacturing systems. The work focused on four threat scenarios that helped the authors analyse the attack of surface of controlled systems and the security risks that arise from their interconnection, operation and expansion with accompanied IIoT devices.
[21]	The work details the factors that have impact on food shortage and agriculture. The authors focus on more as climate change is it has the highest impact when compared to others.
[22]	Focusing on machine vision systems, this work focuses on presenting several types of adversarial threats against deep learning-based computer and presents several approaches to protect against such threats. The work studies a specific model and looks at threats against several use cases such as: human action recognition, crown counting and person reidentification.
[23]	Focusing on machine vision systems, this work focuses on presenting several types of adversarial threats against deep learning-based computer, specifically a framework called INFRASTRESS. The authors also presented several defending mechanisms.

3. Intelligent Harvesting Machines

In order to identify the key components of intelligent harvesting robots, we examined an actual asparagus harvesting robot and also analyzed the architectural design of several harvesting robots in the literature [24–27]. The common elements identified are and summarized in Figure 1:

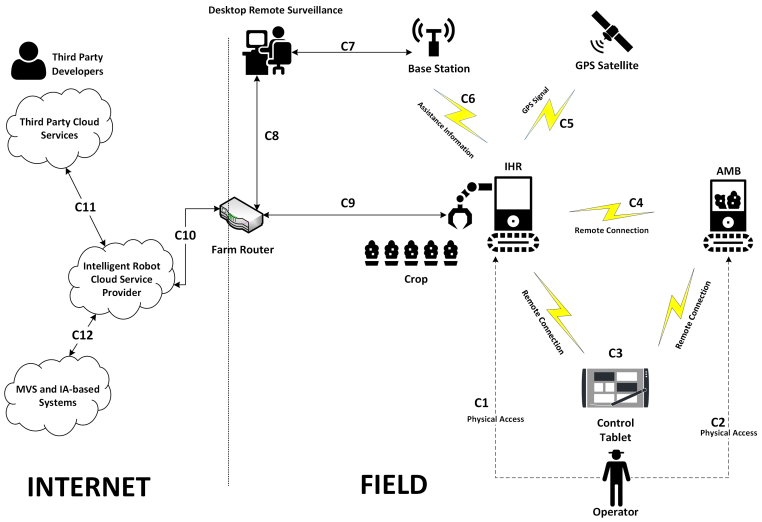

Figure 1. The intelligent harvesting robot system and its key components.

- **Crop** : A trivial component, which might include apple, litchi, citrus, grape, tomatoes, etc. They vary significantly in shape, size, colour texture and other physical,

chemical and nutritional properties. This information is used by the Machine Vision System in the Intelligent Harvesting Robot in order to identify and locate the crop in complex situations.

- **Intelligent Harvesting Robot (IHR)**: The robot is designed to pick fruits/vegetables automatically under certain environmental conditions. It uses a Machine Vision System to accomplish the task of picking the crop under the guidance of visual information. A typical harvesting operation is linked to two sub-tasks:
  1. Automatic Crop Recognition: Also referred to as the Machine Visions System, it means identifying and locating the crop in a natural complex scene.
  2. Eye–Hand Coordination: It focuses on the interaction between the robot visual perception of the work-space and its actuators.
- **Autonomous Mobile Basket (AMB)**: A basket that provides storage to carry the harvested crop. In some cases, the basket is attached to the IHR. In other cases, there is a separate autonomous truck (full of baskets) which follows the robot and supplies empty baskets. Wireless communication is used in both cases.
- **On-Site remote surveillance**: In order to manage and improve the quality of the harvest operation, the farmer can tele-operate both the farming robot and the basket by sending commands through a client application installed on a intelligent device (tablet, smartphone, etc). An example of such commands could be to set the robot to avoid an obstacle or to send the mobile basket to the warehouse to store the harvested crops.
- **Intelligent robot cloud service provider**: The harvesting robot uses cloud services where most of the AI modules and intelligent features reside for further analysis to improve the tasks it performs.
- **Base station**: A GPS receiver that collects GPS measurements of the field. It consists of an antenna, a GPS receiver, and a device (often a personal computer) to which the GPS data is logged. Note that the robot also has a GPS module that collects GPS coordinates from the satellite in order to control its movement, but the difference is that a base station provides reference data that can be used to increase the accuracy (to within a few centimeters or less) of GPS data collected in the field.

The Operator in Figure 1 can interact with the IHR and the AMB by accessing their physical interfaces (this communication is depicted in Figure 1 with dashed lines and labelled (C1) and (C11)) or remotely by sending commands through a client application or a smartphone app (C2 + C3). The IHR essentially executes two tasks in parallel: it collects localisation data from the base station and the GPS satellite (C5 + C6) and also uses image processing to identify crops that are ready for harvesting using the Automatic Crop Recognition task. As soon as a mature plant is detected, access to GPS coordinates is immediately cut off. The robot then moves to the crop to start the harvesting process. Harvesting is conducted by sending a signal to the motor controlling the harvesting blades using the Eye–Hand Coordination task. The blades start as well as the conveyor belt. When the crops are harvested, they are also being transferred into a basket simultaneously. The AMB follows the harvesting robot and continuously checks the IHR's basket (C4). Once the basket is full, the AMB removes it and provides an empty basket. Finally, the AMB will transfer the full basket to the warehouse.

Most of the IHR's intelligent features are developed and maintained in the cloud. For example, the performance of the Automatic Crop Recognition task mentioned before is improved by sending crop images to the Machine Vision System (C12 + C10) in the cloud to train the AI-based model that the robot is using, which then generates the model weights and sends them back to the IHR for inference. The intelligent cloud service provider could also use third party cloud services to enhance the performance of its intelligent modules (C11). An example could be sending the images collected by the IHR to a third-party cloud tool to improve their quality or perform data labeling before sending them to the Machine Vision System.

4. Security and Safety Issues

In this section, we present a classification of the main security and safety issues of intelligent harvesting robots. We use this classification together with the communication labels and components in the architecture described in Section 3 to later categorize current attacks and countermeasures in the next sections.

4.1. Hardware Security Issues

The physical aspect of the robot is probably the first attack vector that attackers or malicious users will try to explore.

4.1.1. Unprotected External/Internal Communication Ports

Robots with unprotected external or internal ports can lead attackers in physical proximity to perform a variety of attacks and serve as an entry point to the robot's file system. Especially if the robot's file system is not encrypted which could leave the average user to be able to recover sensitive or proprietary data off of a storage device or even be able to change code/data of the robot [28]. The attacker could also use the external ports, such as USB ports or an Ethernet port to gain access over IHR or AMB through executing arbitrary commands. There are many examples of USB dongles being used to steal sensitive data or even cause critical to damage the hardware [29]. Another entry point is targeting the unprotected internal communication ports by unplugging sensors, actuators or any robot-related components used in the intelligent harvesting robot. These ports could give the attacker access to the robot's internal network where they can eavesdrop on or disrupt all of the robot's internal communications.

4.1.2. Untrusted Third Party Hardware

In most cases, companies built harvesting robots using hardware that is designed by third party manufacturers. This raises a security and trust issue for the robot itself as some malicious manufactures could purposely leave a backdoor into the robotic system to track and monitor the activities of the robot and its operator without the owner's knowledge. In some cases, they could infect the robot with malware that exploits a deliberate design flaw or configuration to gain unauthorized access to robot data [14]. Another threat is the unauthorised access to the robot's logging system which could contain private data. In this case, this threat takes advantage of inappropriate or missing access control rules in the IHR operating system. The malicious manufacturer could send data to a remote server for example.

4.2. Network Security Issues

This category includes threats that target the external network the IHR use to communicate with external devices (Control Tablet, AMB, etc.). The operator uses short range communication to remotely send commands to both the IHR and the AMB. This is usually conducted via a Wi-Fi access point created by the IHR. Knowing that the wireless communication channel is also used to send storage related data, attackers could launch many attack vectors to break the Wi-Fi network by targeting many areas:

- Attacks targeting communication between IHR/AMB and the Control Tablet: The most critical threat is hijacking the entire communication between the robots and the control table which enables the attacker to connect to the unprotected network and starts eavesdropping information. After sufficient reconnaissance, an attacker then inject new, malicious packets into the network, in order to impact the harvesting operation. The authors in [10] investigated the impact of exploiting wireless vulnerabilities on the actions of tele-operated surgical robots. The study showed that the hijacking, disruption and interception of data on the wireless communication channel can have serious consequences on the robot and the safety of patients and surgeons. For the IHR, this could cause a significant degradation in performance or even unavailability of the system.

- Attacks targeting communication between IHR and the AMB: The Autonomous Mobile Basket constantly or periodically checks the storage state of the portable basket integrated into the Intelligent Harvesting Robot. This also requires a short range communication between both robots. Attackers can disrupt the communication channel by sending special wireless deauthentication packets to both robots (or one of them) to temporarily or even permanently disable them from being able to connect back to the storage system targeting the availability of systems and data. Attackers can also target the confidentiality of data by simply analysing the traffic between both robots. This could be conducted by either passively monitoring the transmitted robotic traffic over encrypted and un-encrypted open communication channels. The aim is to extract sensitive data about the robotic system. Another approach is to actively intercept storage related data and altering it by injecting false data, which deviates the robots from performing their intended activity in an accurate manner, or leave them prone to response delays.
- Attacks targeting communication between IHR/AMB and the Base Station: This set of attack vectors target the localisation and mobility systems of both robots by launching jamming and spoofing attacks. An adversary can jam the wireless sensor and communications producing radio interference to disrupt wireless networks so that the sensors cannot receive GPS related data. Additionally, an adversary can also spoof communications by emitting false signals (e.g., GNSS-like signals, with the intention of producing false location-based information in the victim receiver). Malicious signals can also be exploited to negatively affect the communication channels of wireless sensors. For example, the goal in the latter case may be to deplete battery life or even block the communication channel so that the sensors cannot return their readings. Both examples have a direct impact on availability. This will cause problems to the Automatic Crop Recognition which depend on the target sensor and therefore the associated functionality of IHR/AMB [30].

4.3. Cloud Security Issues

The use of cloud storage and processing services redefines how and where the robotic data are stored and accessed. While cloud technologies offer the advantage of having readily available virtually unlimited resources, they also come with security issues and challenges [18]:

- Unauthorised cloud data access: Cloud services usually offer multiple ways of accessing data (e.g., app- or web-enabled access) which widens the attack service. An attacker can exploit an undiscovered vulnerability and gain access to cloud robot data and then they can read, modify, or even delete any robotic data.
- Third party access: Another important issue is how the developers who create the cloud services connected to IHR/AMB, and who have direct access to any communication channel of the intelligent harvesting machine architecture, protect users from external parties who do not have access to any of these communication channels. In this context, some companies use third-party cloud services that offer additional data processing and analysis to improve the performance of robot services during the harvesting operation. This of course raises another question about how data are shared by those involved in intelligent harvesting machines and what kind of controls and security mechanisms are implemented by third parties to protect shared data.

4.4. System/Software Security Issues

These category involved threats that target systems and software used by IHR to perform daily harvesting operations. An example of these include libraries (for transformation, labelling, etc.), machine learning platforms, visualisation tools and cloud, and the web application used for remote control. Some of these software and tools are internally developed by the company that is building the harvesting robots or belong to a third-party actor. From a security perspective, applications that are not tested and evaluated can have

performance issues and present security vulnerabilities that could be exploited by hackers. Another issue is the lack of constant software and firmware updates that keep the robotic system updated and secure. This could result into having configuration and database vulnerabilities. Additional attack vectors could also be created if AI-based frameworks are not well configured and implemented or managed in the cloud, as this adds an additional layer of complexity.

4.5. AI Security Issues

Depending on the design, the field robots use at least two machine vision systems based on deep learning. The former is used for crop detection, and the latter is used for route planning/obstacle avoidance. Figure 2 illustrates the details of the general machine vision system workflow.

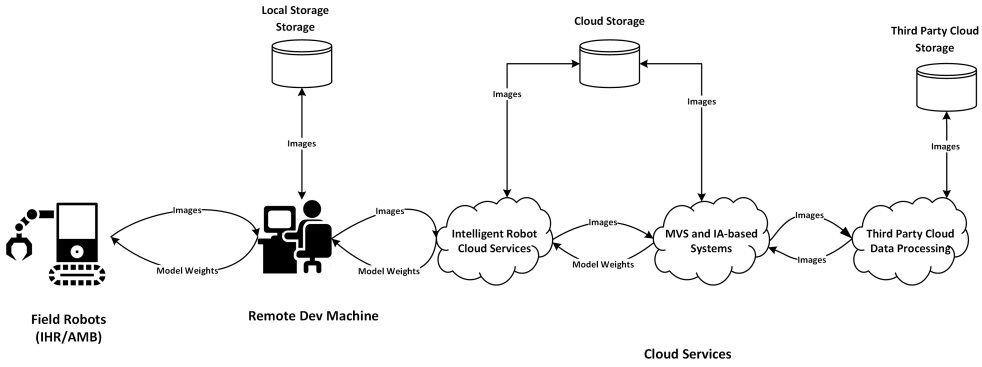

Figure 2. Machine vision system workflow.

As explained earlier, the AI-based systems used by IHR are developed, tuned and maintained in the cloud. The image data collected by the robot is sent to the cloud to improve the performance of the Automatic Crop Recognition module. Note that the quality of these images is evaluated by an intermediate engineer (Remote Dev Machine) before sending it to the MVS. In some cases, companies could also use third-party cloud tools for image cleaning and labeling before training the AI-based system. Additionally, this standard workflow for intelligent harvesting machines have many security concerns that could negatively impact the performance of the AI-based systems. It is wise to keep in mind that AI techniques and systems using AI can lead to unexpected results and can be modified to manipulate the expected results. Decent research has been conducted in identifying the threats to AI-based systems [22,31] and they can be summarised as detailed below:

- Adversarial AI: The aim is to target the inference phase of the ML and deep learning systems in the machine vision system by including perturbations to the crop images that are undetectable to the human eye but maximizes the model's prediction error, forcing it to make wrong predictions.
- Data Poisoning: This involves injecting erroneous/falsified/bad cropping images into the training/validation set by gaining legitimate or illegitimate access by exploiting poor authentication/authorization mechanisms. The purpose is to affect the operation and performance of the machine vision system.
- Input Tampering: By deliberately or unintentionally manipulating crop images in several stages stage of the AI life cycle. Actors such as AI/ML engineers can manipulate data during the storage procedure and using some processes such as feature selection or image labelling. This could interfere with model inference and introduce bias into training data and affect the performance of the machine vision system.
- Model Extraction: These attacks aim to duplicate a machine learning model through query access to a target model. The typical setup for a model extraction attack is an API, such as the ones provided by MLaaS platforms [32]. In the literature, protecting the confidentiality of DLs can be conducted by:

- Change the API to limit the number of user queries and also to ignore incomplete queries,
- Introducing random and controllable noise to the model to maximise the loss of a stolen model while preserving its prediction accuracy. This deceptive perturbation can degrade or slow down the model stealing process.

4.6. Security Gap in Cyber-Physical Systems

During our threat assessment in intelligent harvesting robots, we noticed that the common threat sources provided and recommend by international standards and the community [33–35] do not fully apply to robots and cyber-physical systems. This is because there are certain threat scenarios that cannot be classified into a single category: loss of information systems due to physical damage to the hardware is an example of such threats as it is a combination of a physical and a cyberthreat source. Another example is launching an attack vector that result in physical damage to the robot. Due to the nature of cyber-physical systems, standard threat assessment methods often miss such complex scenarios that can significantly impact robot operation.

5. Impact of the Security/Safety Issues

Lack of appropriate security controls that address the identified threats might have a significant impact on intelligent harvesting companies. This section assesses what would be the impact that would result from threats materialising by focusing on specific use cases.

The use cases will also consider a generic internal design of a intelligent harvesting robot as depicted in Figure 3. This figure also highlights some of the key communication channels with internal and external components:

IHR Critical Assets:

Before assessing the impact of the identified security issues in the use cases, it is necessary to highlight the critical assets in intelligent harvesting architecture described in Figure 1. Assets represent any user, resource (for example, disk space) or property (for example, the physical security of users) of the system. They also have properties that can be linked to the achievement of IHR's business goals. For example, IHR data stores are a resource/asset of the system, and the confidentiality of that data is a system property and a business goal for companies in intelligent harvesting. Table 2 highlights the IHR's critical assets and their corresponding CIA (or Confidentiality, Integrity and Availability) attributes that must be maintained.

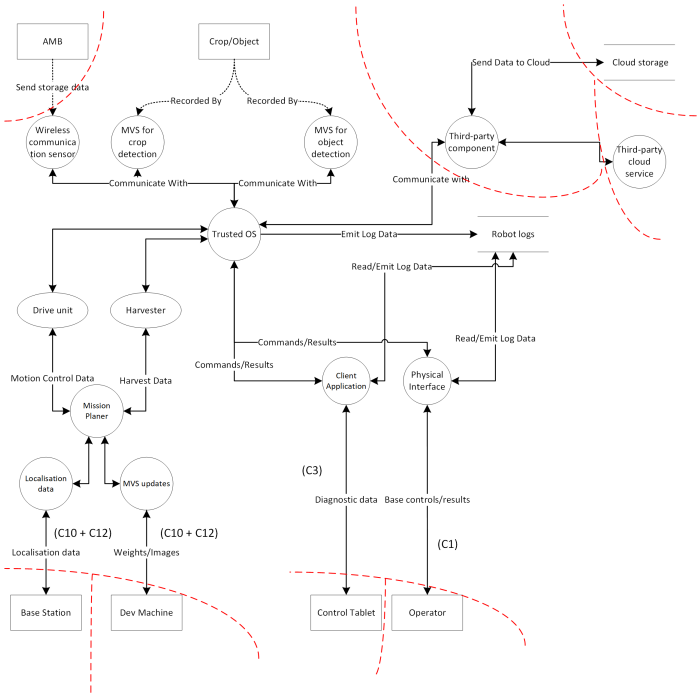

Figure 3. Data Flow Diagram of the IHR.

Table 2. Critical Assets of IHR from a Security Perspective.

Asset/Resource		CIA Triad		
Type	**Description**	**Confidentiality**	**Integrity**	**Availability**
Sensors and camera data	Any data produced by the sensors should be accessed and available to the authorised actors.	✓		✓
IHR Data Stores	IHR persistent data (logs, software, etc.) must be accessible to only authorised actors.	✓	✓	
Physical safety	IHR system must not harm its users or environment		✓	
IHR Behaviour	The robotic system must not allow attackers to disrupt its tasks		✓	
Compute Capabilities	Robot embedded and distributed (e.g., cloud services) compute resources. The unavailability the compute resources of IHR and the MVS will prevent the robot from operating correctly			✓
IHR	The IHR must not damage itself and must respond to commands within a reasonable time.		✓	✓

5.1. Use Cases

This section presents three use cases that are carefully selected after analysing several threats in the intelligent harvesting environments. The aim is to give the reader a deeper insight into the type of critical threats that can harm intelligent harvesting robots and even their operators.

Use case 1: adversarial perturbation against the machine vision system

The first use case is about introducing physical disturbances to the crop to deceive the sensors of the intelligent harvesting robot into perceiving erroneous information about the

environment. The adversarial attacks are crafted after performing several experiments to successfully confuse the MVS. An example of these changes could be:

- placement of objects;
- deformation of the crop;
- changing external environmental factors (projection of light on the crop).

The attack steps are summarized as follows:

1. The attacker starts by analysing the capabilities of the targeted versions of the cameras and the MVS.
2. The adversary designs an adversarial attack capable of altering the outputs. This is a trial-and-error phase it requires many physical experiments and disturbance models to increase the success rate of the attack.
3. The attacker launches the attack by performing the alteration on the crop to cause misclassification by IHR.
4. When IHR arrives at the targeted location, it will erroneously classify it into the attacker's chosen class (e.g., interpret a ripe asparagus as unready) and react accordingly (e.g., ignores instead of harvesting).

Use case 2: Sensor/communication jamming and GPS spoofing

An attacker can disrupt wireless sensor communication by producing radio interference. The aim is to prevent sensors from receiving GPS positioning and correction messages. The attacker can also spoof communications by emitting false signals (e.g., GNSS-like signals, with the intention of producing false location-based information in the victim receiver). Malicious signals can also be exploited to negatively affect the communication channels of wireless sensors. The attack steps are summarized as follows:

1. Security vulnerabilities in sensors and GPS signals are identified.
2. Taking advantage of the vulnerable sensors, the adversary remotely injects unwanted signals into the communication channel or disables sending/receiving messages.
3. The attacker will use the compromised sensor to block or disrupt the dara transmission, which will affect the functionality of the decision algorithms that IHR uses to perform its normal operation. If the GPS is spoofed, the intelligent harvesting robot will receive erroneous data which will confused its Machine Vision System.

Use case 3: Swapping or using malicious hardware components

The last use case is when attackers utilize malicious hardware components in the IHR/AMB. The hardware is specifically designed to support attacks by attaching a virus or a trojan that is programmed to send personal data to the remote attacker for example. The attack steps are summarized as follows:

1. Attacker starting by analysing the robot hardware design to identify internal hardware that is accessible from outside such as sensors, actuators, computation units, user interfaces, etc.
2. Attacker disable or remove accessible components and plug malicious new ones
3. Attacker implement back-doors to gain unauthorized access to the robots

5.2. Threat Impact Assessment

This subsection assess the technical (Table 3) and financial impacts (Table 4) of the identified uses cases. The degree of the impact depends on many factors such as the severity of the vulnerability, the value of the assets, etc.

Table 3. Technical impact of the studied use cases.

Use Case	Impact	Impacted Asset					
		Sensors/Camera Data	IHR Data Stores	Physical Safety	IHR Behaviour	Compute Capabilities	IHR
Use Case 1	Missclassification of images which might results to ruining, crushing, or ignoring crops	✓		✓	✓	✓	✓
	Unstable navigation function in the drive unit if perturbations were introduced to the path of IHR	✓		✓	✓		✓
	Integrity of data is compromised in case of poisoning images with adversarial data sets			✓	✓	✓	✓
Use Case 2	Battery life is depleted due unstable situational awareness and the robot's navigation function				✓	✓	
	Communication channels are blocked due jamming and denial of service attacks	✓			✓	✓	✓
Use Case 3	IHR and users are under constant surveillance, monitoring, and tracking due to an installed backdoor	✓	✓				
	Malicious and dangerous behaviour of IHR: the intelligent harvesting drives through farmers or throws itself into into a hedge or a ditch because of a remote access attack		✓	✓			✓

Generally speaking, attacks on intelligent harvesting robots can either have an immediate (operational) effect or a future (business) effect that includes financial and market consequences. Examples of each impact is described in the table below:

Table 4. Financial and operational impacts of the studied use cases.

Impact	Type	Example
Business	Direct	The financial replacement value of lost (part of) asset.
		The cost of acquisition, configuration and installation of the new asset or backup.
		The cost of suspended operations due to the incident until the service provided by the asset(s) is restored.
		Impact results in an information security breach.
	Indirect	Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere);
		The cost of interrupted operations.
		Potential misuse of information obtained through a security breach.
		Violation of statutory or regulatory obligations.
		Violation of ethical codes of conduct.
	Long term	Loss of reputation (Trustworthiness).
		Loss of public confidence (Trust).
		Tarnished image of PSA and of the Government.
		Potential legal action if privacy legislation is breached.
		Privacy Loss if it is possible to correlate identities across processes or make inferences from aggregated data sets
Operational	Field Robot	Significant degradation in performance of the machine vision system and AI-based modules (e.g., crop detection, path planning, etc.)
		Unexpected behaviour of IHR/AMB
		Delays in decision making and unavailability of data and services
		Exposure of data-sets and sensitive information
		Loss of data/code of the harvesting robot.

6. Conclusions

Using intelligent robots in farms to help with crop planting and harvesting comes with great benefits to the farmer. However, as robotic systems pose an increased risk of several security issues that can be exploited to launch dangerous attacks, intelligent farming will also suffer from dramatic consequences ranging from economic losses to loss of human lives.

In this context, we examined a real asparagus harvesting robot and evaluated its security; the proposed architecture was the result of our threat analysis and from studying other intelligent harvesting architecture systems in the literature and industries. This paper identified all security and safety threats that surround each key component in the architecture and classified them into five categories: network, hardware, software, AI and cloud security issues. For example, the category of network security issues describes several attacks on the confidentiality, integrity and availability of robotic data and services. We also pointed out that some attack vectors cannot be categoried into a single category due to the complex nature of cyber-physical systems. At the end of the article, we look at three specific use cases and analyze the stages of attacks and the impact of each scenario. These attacks target the machine vision system, GPS communication channels and hardware use by the robot. A successful attack on the machine vision system will cause the robot to engage in unpredictable behavior that can lead to human injury. That is why we considered the first two cases as one of the most serious threats to intelligent harvesting robots. As part of

our future work, we plan to analyze more attack scenarios on the intelligent harvesting system with more emphasis on countermeasures to mitigate the risks of compromising the integrity, confidentiality and availability of intelligent harvesting robots.

Author Contributions: Conceptualization, N.M., G.E. and C.M.; methodology, N.M., G.E.; Data, C.C. and J.M.; validation, N.M., G.E., C.M., C.C. and J.M.; formal analysis, N.M.; investigation, N.M.; resources, C.C. and J.M.; writing—original draft preparation, N.M.; writing—review and editing, N.M., G.E.; supervision, G.E. and C.M.; project administration, G.E. and C.M.; funding acquisition, C.M. and C.C. All authors have read and agreed to the published version of the manuscript.

Funding: The work presented has been funded by Grant 97167 (Muddy Machines) through UK Research and Innovation (UKRI) under the Building Resilient Robotic Harvesters for High Value Field Vegetables project.

Data Availability Statement: Data supporting this study cannot be made available due to legal and commercial reasons.

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

Abbreviations

The following abbreviations are used in this manuscript:

AMB	Autonomous Mobile Basket
API	Application Programming Interface
GPS	Global Positioning System
AI	Artificial Intelligence
IoT	Internet of Things
ML	Machine Learning
MVS	Machine Vision System
IHR	intelligent harvesting Robot

References

1. Etspeaksfromhome. Teksta Robotic Puppy Review. Available online: https://etspeaksfromhome.co.uk/2014/10/teksta-robotic-puppy-dalmatian-review.html (accessed on 1 November 2022).
2. Right, R.D. Assembly Line Robots. Available online: https://robotsdoneright.com/Articles/assembly-line-robots.html (accessed on 30 October 2022).
3. QinetiQ. MAARS Weaponized Robot. Available online: https://www.qinetiq.com/en-us/capabilities/robotics-and-autonomy/maars-weaponized-robot (accessed on 29 October 2022).
4. IFR—International Federation of Robotics. World Robotics 2020 Report. *Int. Fed. Robot.* **2020**, *49*, 16–18.
5. Fahmida Islam, S.; Uddin, M.S.; Bansal, J.C. Harvesting Robots for Smart Agriculture. In *Computer Vision and Machine Learning in Agriculture*; Uddin, M.S., Bansal, J.C., Eds.; Springer: Singapore, 2022; Volume 2, pp. 1–13. [CrossRef]
6. Lovett, I. Robots Take Over Italy's Vineyards as Wineries Struggle with COVID-19 Worker Shortages. *The Wall Street Journal*, 3 October 2022.
7. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2021**, *21*, 115–158. [CrossRef] [PubMed]
8. Vilches, V.M.; Kirschgens, L.A.; Calvo, A.B.; Cordero, A.H.; Pisón, R.I.; Vilches, D.M.; Rosas, A.M.; Mendia, G.O.; Juan, L.U.S.; Ugarte, I.Z.; et al. Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics. *arXiv* **2018**, arXiv:1806.04042.
9. Colell, A. Hacker Report: Understanding Hacker Motivations, Development and Outlook. In *Energiepolitik und Klimaschutz. Energy Policy and Climate Protection*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 257–282. [CrossRef]
10. Bonaci, T.; Herron, J.; Yusuf, T.; Yan, J.; Kohno, T.; Chizeck, H.J. To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots. *arXiv* **2015**, arXiv:1504.04339.
11. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* **2020**, *20*, 6458. [CrossRef] [PubMed]
12. Morante, S.; Victores, J.G.; Balaguer, C. Cryptobotics: Why Robots Need Cyber Safety. *Front. Robot. AI* **2015**, *2*, 23. . [CrossRef]
13. Bhardwaj, A.; Avasthi, V.; Goundar, S. Cyber security attacks on robotic platforms. *Netw. Secur.* **2019**, *2019*, 13–19. [CrossRef]
14. Alemzadeh, H.; Chen, D.; Li, X.; Kesavadas, T.; Kalbarczyk, Z.T.; Iyer, R.K. Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation. In Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016, Toulouse, France, 28 June–1 July 2016; pp. 395–406. [CrossRef]

15. Kazanzides, P. Safety Design for medical robots. In Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009, Minneapolis, MN, USA, 3–6 September 2009; pp. 7208–7211. [CrossRef]
16. Vuong, T.; Filippoupolitis, A.; Loukas, G.; Gan, D. Physical indicators of cyber attacks against a rescue robot. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM Workshops 2014, Budapest, Hungary, 24–28 March 2014; pp. 338–343. [CrossRef]
17. Cerrudo, C. Hacking Robots Before Skynet 1. In *Cybersecurity Insight*; IOActive, Inc.: Seattle, WA, USA, 2017; pp. 1–17.
18. Suarez-tangil, G. Smart Home Personal Assistants: A Security and Privacy Review. *ACM Comput. Surv.* **2019**, *53*, 1–36.
19. Aldinhas Ferreira, M.I.; Fletcher, S.R. (Eds.) *The 21st Century Industrial Robot: When Tools Become Collaborators*; Springer: Cham, Switzerland, 2022; Volume 81, pp. 1–286.
20. Pogliani, M.; Quarta, D.; Polino, M.; Vittone, M.; Maggi, F.; Zanero, S. Security of controlled manufacturing systems in the connected factory: The case of industrial robots. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 161–175. [CrossRef]
21. Calicioglu, O.; Flammini, A.; Bracco, S.; Bellù, L.; Sims, R. The Future Challenges of Food and Agriculture: An Integrated Analysis of Trends and Solutions. *Sustainability* **2019**, *11*, 222. [CrossRef]
22. Kafali, E.; Zafirouli, K.; Karageorgos, K.; Semertzidis, T.; Daras, P. 2. Cyber-physical Adversarial Attacks and Countermeasures for Deep Learning Vision Systems on Critical Infrastructures. In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*; Now Publishers: Boston, MA, USA; Delft, The Netherlands, 2021; pp. 22–50. [CrossRef]
23. Hasan, M.M.; Islam, M.U.; Sadeq, M.J. Towards technological adaptation of advanced farming through AI, IoT, and Robotics: A Comprehensive overview. *arXiv* **2022**. [CrossRef]
24. Kootstra, G.; Wang, X.; Blok, P.M.; Hemming, J.; van Henten, E. Selective Harvesting Robotics: Current Research, Trends, and Future Directions. *Curr. Robot. Rep.* **2021**, *2*, 95–104. [CrossRef]
25. Li, J.; Tang, Y.; Zou, X.; Lin, G.; Wang, H. Detection of Fruit-Bearing Branches and Localization of Litchi Clusters for Vision-Based Harvesting Robots. *IEEE Access* **2020**, *8*, 117746–117758. [CrossRef]
26. Zhou, H.; Wang, X.; Au, W.; Kang, H.; Chen, C. Intelligent robots for fruit harvesting: Recent developments and future challenges. *Precis. Agric.* **2022**, *23*, 1856–1907. [CrossRef]
27. Tang, Y.; Chen, M.; Wang, C.; Luo, L.; Li, J.; Lian, G.; Zou, X. Recognition and Localization Methods for Vision-Based Fruit Picking Robots: A Review. *Front. Plant Sci.* **2020**, *11*, 510. . [CrossRef] [PubMed]
28. McClean, J.; Stull, C.; Farrar, C.; Mascare nas, D. A preliminary cyber-physical security assessment of the Robot Operating System (ROS). *Unmanned Syst. Technol. XV* **2013**, *8741*, 874110. [CrossRef]
29. Singh, T. Top 5 Usb Hacks that Pwn You. Available online: https://geeknizer.com/top-usb-hacks-pwn/ (accessed on 15 November 2022).
30. European Union Agency for Network and Information Security. *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*; ENISA: Athens, Greece, 2021.
31. Malatras, A.; Dede, G. *Artificial Intelligence Cybersecurity Challenges—ENISA*; ENISA: Athens, Greece, 2020.
32. Florian, T.; Fan, Z.; Ari, J.; Michael, K.R.; Thomas, R. *Stealing Machine Learning Models via Prediction APIs*; USENIX Association: Berkeley, CA USA, 2016.
33. James, T.; Kelli, K.T. *Open Threat Taxonomy*, Version 1.1; Technical Report. Available online: https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf (accessed on 12 October 2022).
34. *ISO/IEC 27005*; Information Technology—Security Techniques—Information Security Risk Management. Technical Report; Joint Technical Committee: Geneva, Switzerland, 2011.
35. NIST. *NIST Special Publication 800-30: Guide for Conducting Risk Assessement*; Technical Report; NIST: Gaithersburg, MD, USA, 2012.