Energy Nexus 14 (2024) 100300

Contents lists available at ScienceDirect

Energy Nexus

journal homepage: www.elsevier.com/locate/nexus

Leveraging precision agriculture techniques using UAVs and emerging disruptive technologies☆

Meghna Raj [a], Harshini N B [a], Shashank Gupta [a,*], Mohammed Atiquzzaman [b], Oshin Rawlley [a], Lavika Goel [c]

[a] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India
[b] School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA
[c] Department of Computer Science and Engineering,Malaviya National Institute of Technology Jaipur, JLN Marg, Jaipur, Rajasthan 302017, India

ARTICLE INFO

Keywords:
Unmanned aerial vehicles
Precision agri- culture
Smart farming
Internet of things
Cyber Attacks
Blockchain
Machine Learning
Artificial Intelligence

ABSTRACT

The next great innovation in Unmanned Aerial Vehicles (UAV) technology is smart UAVs, which aim to provide new possibilities in numerous applications. There is an increasing usage of UAVs in various fields of civil applications including live tracking, wireless connectivity, distribution of goods, remote sensing, protection and surveillance, precision agriculture, and review of civil infrastructure. UAVs or drones have a tremen- dous potential to provide smart farming with various productive solutions. Internet of Things (IoT) technologies together with UAVs are anticipated to transform agriculture, allowing decision- making in days rather than weeks, offering substantial cost savings and yield increases. These technologies are employed in a number of different ways, from monitoring crop status and amount of moisture in soil in real time to using drones to help with activities such as the application of pesticide spray. Nonethe- less, the employment of such IoT and smart networking technol- ogy, exposes the smart farming ecosystem to cyber security risks and vulnerabilities. This survey gives a detailed understanding of UAV applications in Precision Agriculture (PA). In this survey, we demonstrate a comprehensive analysis on security and privacy in a smart farming scenario. In this complex and dispersed cyber- physical environment, we describe how Blockchain technology along with 5 G in UAVs communication network can dissipate the security issues of the network. The survey addresses possible scenarios for cyber threats and the advancement in the fields of machine learning and artificial intelligence that can boost cybersecurity. At last, the survey outlines open research issues and future directions in the field of cybersecurity in UAVs and PA.

1. Introduction

The technological advancement in the fields of biology, robotics, and chemistry has made a major contribution to the emergence of technology in agriculture. However, pri- marily owing to the inexorable growth of the worldwide population, agricultural commodities ought to be increased significantly. As per [1], agricultural goods need to be raised by 70 percent by 2050, when the population of the world is projected to touch 9 billion. The agriculture industry must tackle major problems, such as climate change issues, the dwindling supply of arable land and the increasing demand for freshwater simultaneously. The services from Information and Communication Technology (ICT) can provide realistic workarounds for these prominent issues. More precisely, the emergence of the Internet of Things (IoT) and, in particular, the rapid advancement of technologies for unmanned aerial vehicles (UAV) coupled with image data analytics can offer exciting strategies for Precision Agriculture (PA) to overcome the above obstacles. In addition, PA attempts to implement ICT resources to integrate and analyze knowledge supplied by numerous outlets that can help draw valuable insights about the understanding of the soil, making it possible to control crops more effectively [2]. UAVs have grown very popular in our day to day lives with the advancements in technology and will continue to have major influence in the foreseeable future [3]. In the coming years, the quantity of UAVs used for civilian and commercial purposes is projected to grow exponentially across the world. The total number of UAVs registered in the United States reached one million in January 2018, as per the Federal Aviation

☆ Digital Object Identifier: XXXXXXXXXXXX
* Corresponding author.
E-mail address: shashank.gupta@pilani.bits-pilani.ac.in (S. Gupta).

https://doi.org/10.1016/j.nexus.2024.100300
Received 23 July 2023; Received in revised form 12 March 2024; Accepted 15 April 2024
Available online 20 April 2024

Administration (FAA), and will exceed 4.3 million by 2020. In addition, more and more UAV applications are predicted to emerge, which include those that are prevalent to the general populace, such as the usage of UAVs for infotainment and distribution, a few that are utilized in specific contexts, such as the use in land surveys, PA, emergency response, etc., as seen in Fig. 1. Numerous different UAV functions need to be designed and implemented in order to build a UAV application. For instance, Fig. 1. indicates that a drone lighting display application involves a variety of functions, such as a path planning function to decide the direction of UAVs as per a choreographic pattern, a positioning functionality for UAVs to recognize their specific locations, some UAVs to fly on the expected path and to land safely according to flight control and power management functions. Furthermore, for management and teamwork, the application can include functions for communication and networking.

1.1. UAV-Based airborne computing for precision agriculture

A PA application has been included in this subsection as an example to illustrate the development of a UAV application and the integration of airborne computing.

Analysis and Design: The analysis and design has been extended to the three-layer reference model. From Fig. 2., we can see that the mission layer of the model has one mission. The task layer has two tasks, which are land survey and pre- cision spraying. There are six functions in the function layer. The task of land surveying involves numerous functions. The entire task is divided into three stages. The first stage ascertains the function of completely covering a particular geographical area by a surveying UAV, with the usage of an algorithm for path planning. The positioning function of the UAV must be triggered for launching the UAV for surveying. This must be done for comprehending the current location of the UAV and a scheme to allow the control of the trajectory, which is to be accomplished by the uploaded path information to the UAV. Then, a photo capturing process will take place during the survey phase, in which images will be taken by the UAV pointing to the ground and the location information will be provided in the metadata of the photos. The images are downloaded in the second stage, when the UAV returns after survey. A ground station will use a 3D mapping [4] application to process the photos and create a 3D map for the area. In order to evaluate the 3D direction for each agricultural UAV, another

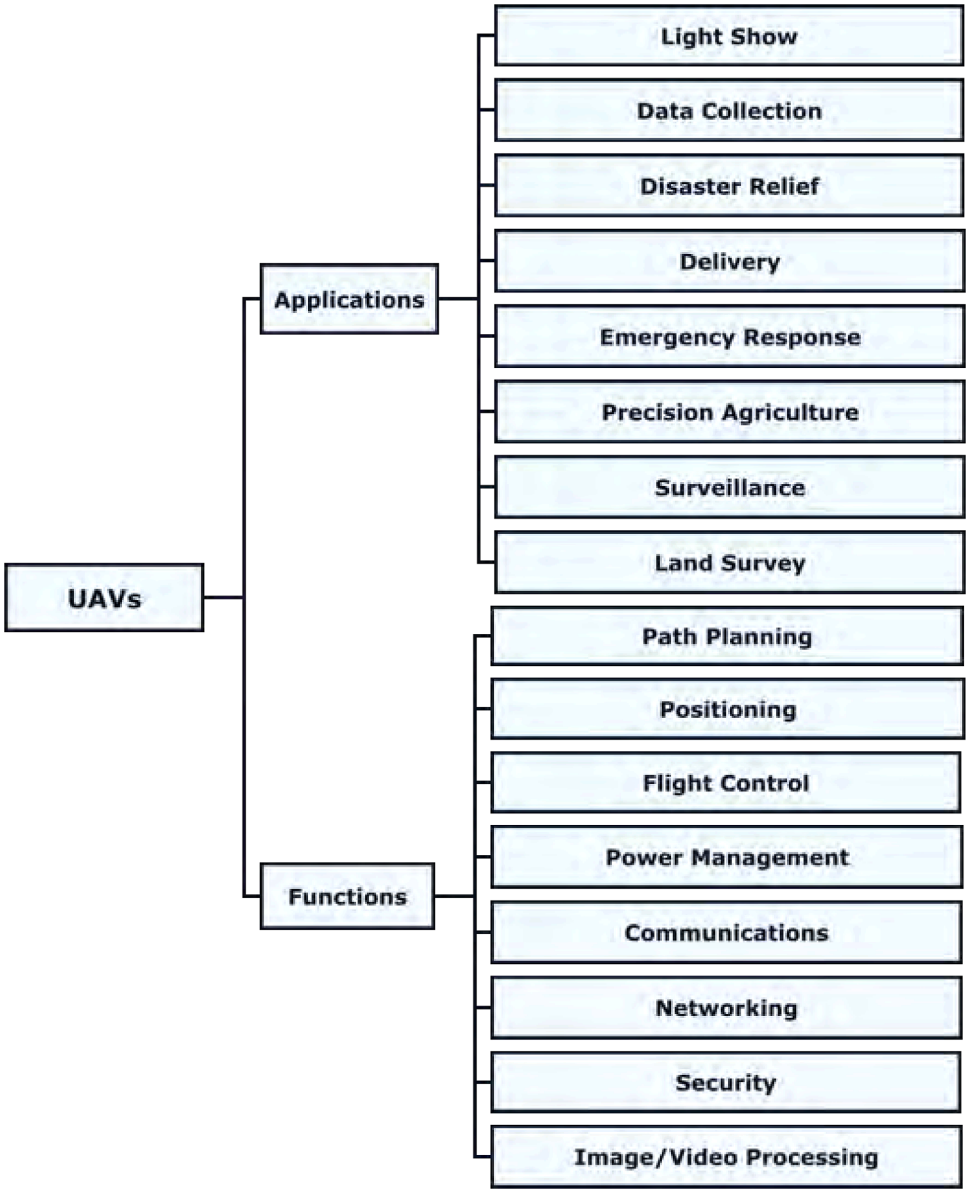

Fig. 1. A few applications and functions of UAVs.

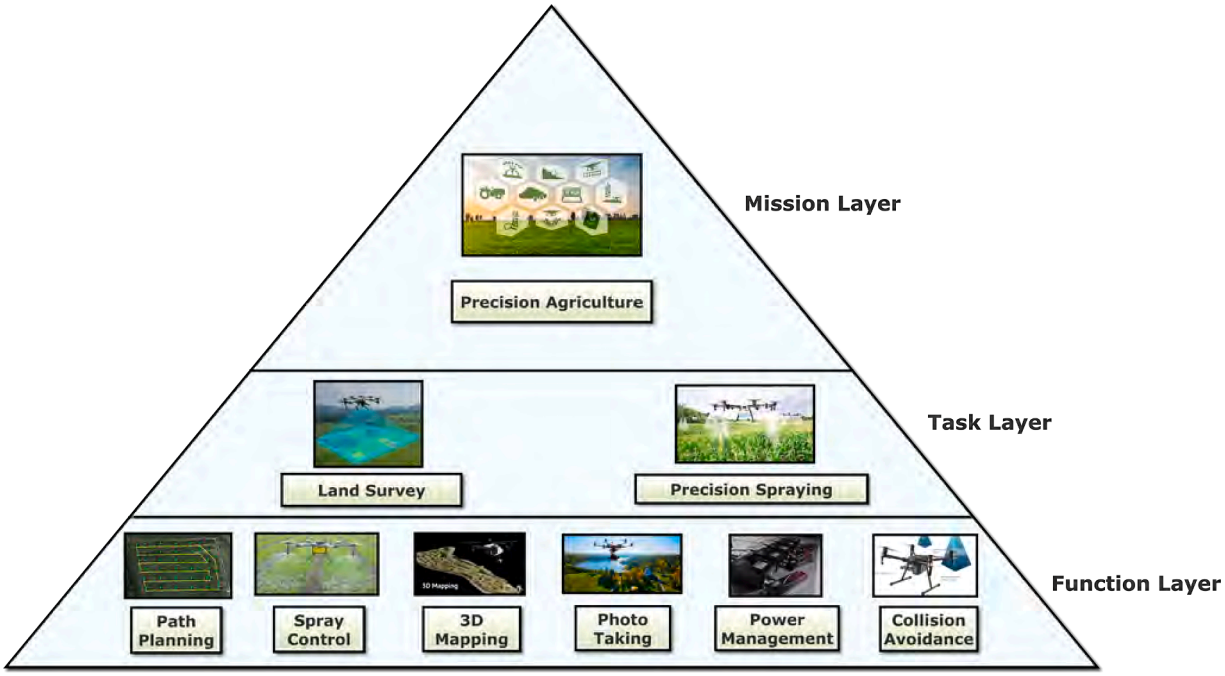

Fig. 2. Layered view of UAV-based precision agriculture.

path planning algorithm will be performed. In the next step, after the path information is submitted to each agricultural UAV, its positioning feature and the trajectory control algorithm will be triggered accordingly. In addition to these functions, UAV farming may allow a terrain matching scheme to enhance spray performance, such as stopping exactly 5 metres above a tree, and may also allow a collision avoidance function to ensure the protection of UAVs and land units.

UAV-Based Airborne Computing: We can easily define many UAV functions from the above discussions that involve airborne computing, including targeting, trajectory monitoring, landing, power management, terrain matching, avoidance of collisions, and control of sprays. Although several of the above functions have been used in current frameworks, through leveraging airborne computing, realisation of more functions can be made possible. For instance, to further increase the precision and reliability of positioning, we can use a UAV's computing capabilities. On the other hand, during the flight assignment, we can also use airborne computation to create 3D maps. In addition, we would be able to develop new schemes based on the 3D maps to dynamically change the trajectory of a surveying UAV to boost the 3D maps.

1.2. Security aspects of UAVs and smart farming

UAV connectivity has now become a core research field that draws researchers around the world and targets scala- bility of coverage, increased throughput, and security. UAVs may transfer or exchange information amongst themselves for scalability, reliability, and accuracy outcomes, in multi- UAV systems. UAVs can be monitored or guided via the air interface by a base station and UAVs can send analysed data for reliable and consistent results to the base station. If there is a deviation of UAV from the line of vision, satellites which can act as a base station and are used for the detection of UAVs. In order to safeguard UAVs against jamming, eavesdropping, hijacking, etc., researchers have begun investigating potential cyber-attacks and their mitigation strategies. Blockchain (BC) technology requires the integration of cryptographic methods with UAVs for the establishment of safe communication and utilization in various applications, such as security and commercial applications. As it eliminates the security threats related with UAV communication it is being embraced by several industries. This has contributed to greater UAV involvement in the BC network, but owing to latency and scalability problems, existing communication networks are immune. UAV connectivity is created to be more secure against vulnerabilities in the network by the combination of BC and 5 G for security and for communication respectively.

By incorporating on-field mobile sensors and equipment, smart farming advances traditional farming practices. These sensors and devices operate synergistically to have accurate farming experience, as well as to increase crop yields. Al- though advantageous to the industry's productivity, possible cyber threats and vulnerabilities in the agriculture sector have been revealed by the use of heterogeneous, internet- connected devices. Such attacks make it possible to control and manipulate on-field sensors and autonomous vehicles remotely (aerial vehicles, tractors, etc.). A dangerous and unproduc- tive farming climate may be created by possible agricultural attacks. Cyber assaults on smart farming systems can have significant effects for many players in the environment, if not constantly controlled. These classes include producers, end-users, food processing companies, cooperatives of agriculture, cattle, government departments, and agriculture-critically de- pendent countries.

1.3. Key contributions of the survey

The prior researches certainly make a substantial contribu- tion to the relationship between UAV services and agricultural development by addressing specific applications, future prob- lems, methodologies and open concerns. Nevertheless, neither of them gives a thorough analysis evaluating individual UAV applications in the PA domain in depth. Several of the research articles on the different security elements of the UAV network have been written by different scholars to date. Most of the articles, as per the information of the reviewers, concentrated on one or a few selected security problems and did not examine BC's suitability for UAV contact. However, there is no systematic survey that takes into account all potential security flaws of the UAV communication system. There is now a possibility of in-depth research on secure smart cars, IOT devices, edge cloud, drones, wireless networking which can be extended to the field of smart farming. The key contributions of our survey are as follows:

- This survey aims at delivering a detailed survey, which explores in depth 20 UAV applications pertaining to PA.
- The survey understudies the background of the BC technology, UAV communication, 5 G network, and their combination, together with the classification of security issues in 5G-enabled UAV.
- It highlights possible smart farming cybersecurity prob- lems and explains cyber attacks specific to particular scenarios that have been classified into data, supply chain, network, and other typical attacks.
- It offers a clear vision of the complexities of open security research in numerous fields, including security for the next generation network, reliable distribution network and regulation, adversarial artificial intelligence and machine learning, and access management, trust and exchange of knowledge.

1.4. Outline of the survey

The rest of the paper is organized as follows. In Section 2, we talk about the types of UAVs, and the applications of UAVs in PA. An overview of various UAV sensors employed in PA is provided, along with the various deep reinforcement learning techniques in UAVs applications and energy harvesting tech- niques that are used in UAVs. In Section 3, we examine the security and privacy concerns of 5 G communication network integrated with UAVs and provide a detailed analysis of them. We offer an in-depth study of the research problems of BC's alignment with the futuristic communications system of UAVs. Section 4 discusses numerous onslaughts on smart farming environment, which includes the supply chain component. Current studies and state of the art on the safety of smart farming are discussed. The chapter highlights open issues in research and viable paths to solutions. Finally, the paper is concluded in Section 5. In order to convey a clear presentation, the organizational structure of the paper is exhibited in Fig. 3.

2. Overview of UAVS and their applications in precision agriculture

The UAV is an aircraft capable of flying independently without a pilot being present. The UAV flight plan is typically pre-defined, or a pilot may monitor its movement and trajec- tory from a ground control station by remote teleoperation commands [5]. In the 21st century, starting with World War I, this technology developed rapidly, the first initiatives to deploy UAVs were undertaken for military purposes. In particular, Dayton-Wright Airplane Company designed an unmanned aerial torpedo that was capable of exploding at a predefined time [6]. An autonomous torpedo able to burst at a particular moment in 1917 was also developed by the Hewitt-Sperry Automatic Airplane company [7]. The first impressive de- ployment and use of UAVs was achieved in World War II, when Reginald Denny Industries designed fifteen thousand UAVs intended for the US Army. The Cold War helped in promoting the production of UAVs as well. The MQM-57 Falconer was used in particular for a scouting operation in 1955 [6]. In addition, in the 1982 Lebanon War, Israel used UAVs as scouting devices, jammers and decoys. Likewise, the Predator RQ-1 L UAV was used in the Balkan War. A graphical representation of the drones used during the wars is given in Fig. 4. Finally, new military campaigns, for instance, the wars in Iraq, Afghanistan, and Syria have also adopted UAVs. While the first UAVs were used mainly in military operations, there is a rapid development of modern technologies such as Inertial Measurement Units (IMU) [8], imaging sensors, and Synthetic Aperture Radar [9]. Global Navigation Satellite Systems (GNSS) [10] have contributed to the evolution of civilian UAVs competent of supporting development of various fields, such as PA, geoinformatics, logistic support and surveillance of infrastructure. Civilian UAVs have two main classes: a) fixed-wing and b) rotary-wing or multirotor. In the following subsections, both groups will be further analysed. The milestones were achieved by the Sensefly company for fixed- wing UAVs, developing efficient UAVs for PA applications [6]. Microdrones, on the other hand, produced the first rotary-wing UAV. The aim of this section is to provide a concise impression of UAV technology by describing the various types of UAVs, their characteristics, their possible payloads, and the regulatory circumstance of their use in Europe. It should be explained at this stage that the technological aspects of the UAV pertain to the features needed for its operation, while the payloads attribute to the supplementary tools used for other purposes, like monitoring.

2.1. UAV types based on aerodynamic features

UAVs can be divided into three groups based on aerody- namic characteristics: a) fixed-wing, b) rotary-wing and c) hybrid [11]. The fixed-wing has a well defined static and fixed wing airfoil that allows lifting based on the forward UAV airspeed. This type of UAV is

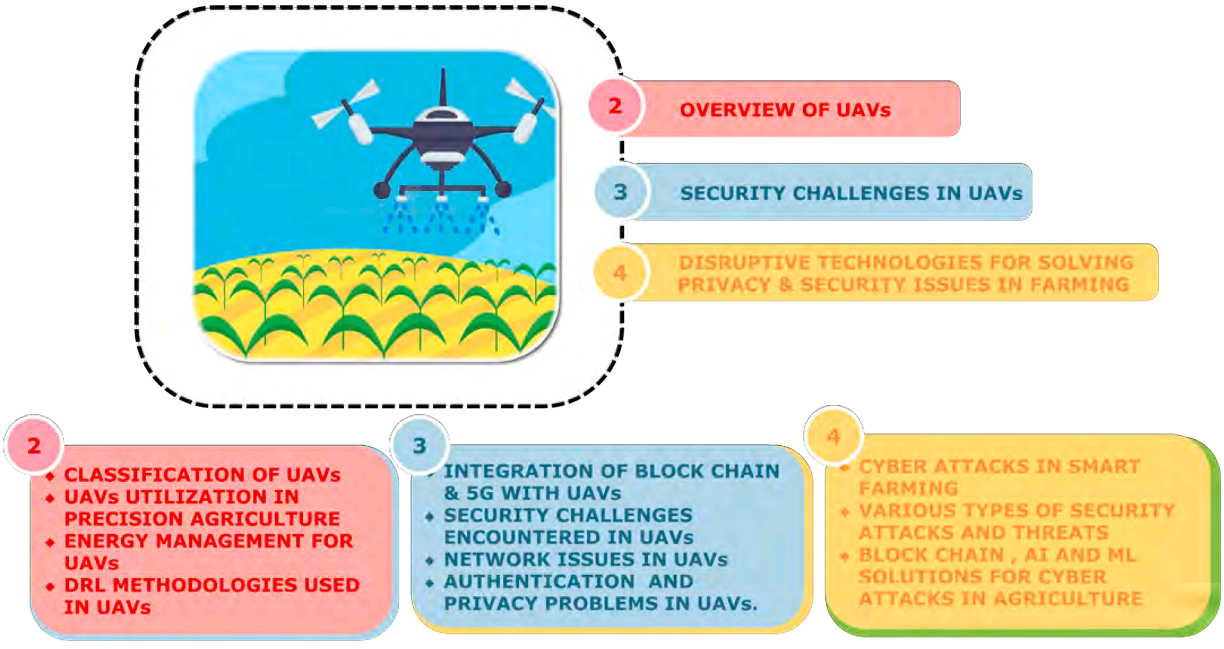

Fig. 3. Outline of the survey.

SENSOR TYPE	FREQUENCY OF OPERATION	APPLICATIONS	DISADVANTAGES
 DIGITAL CAMERA	Visible region	• Visible properties • Outer defects • Greenness • Growth	• Limited to visual spectral bands and properties
 3D CAMERA	Infrared laser region	• Physical attributes • Plant height • Canopy destiny	• Lower accuracies • Limited field applications
 HYPERSPECTRAL CAMERA	Visible infrared region	• Plant stress • Produce quality • Safety control	• Image processing is challenging
 LiDAR	Laser region	• Accurate estimates of plant or tree height and volume	• Sensitive to small variations in path length
 MULTISPECTRAL CAMERA	Visible infrared region	• Responses to nutrient deficiency • Water stress • Plant diseases	• Limited to few spectral bands
 SONAR	Sonar propagation	• Mapping and quantification of the canopy volumes • Digital control of application rates in sprayers or fertilizer spreader	• Sensitivity limited by acoustic absorption, background noise • Lower sampling rate than laser-based sensing
 SPECTROMETER	Visible near infrared region	• Detecting disease • Detecting stress and crop responses	• Background such as soil may affect the data quality • Possibilities of spectral mixing • More applicable for ground sensor systems
 THERMAL CAMERA	Thermal infrared region	• Stomatal conductance • Plant responses to water stress and diseases	• Environmental conditions affect the performance • Very small temperature differences are not detectable • High resolutions cameras are heavier

Fig. 4. Some Unmanned Aerial Vehicles sensors used in precision agriculture for monitoring and data collection purposes.

controlled by means of wings connected to the elevators, ailerons and rudder. In particular, these construction features allow UAVs to turn around angles of roll, pitch and yaw, respectively. The second form of airflow (rotary-wing) consists of numerous rotors which produce the suitable power required for lifting. This form is different from a fixed-wing in the sense that it does not need a forward airspeed for lifting. This UAV is therefore controlled by the torque and propel of the rotors. For example, the diagonal rotors' speed determines the movement of the yaw. More precisely, the rotary-wing UAV can be categorised into the following groups based on the number of rotors: a) tricopter, b) quad-copter, c) hexacopter and d) octocopter. The various kinds of UAVs are shown in Fig. 6. It is noteworthy that the corresponding pros and cons are present in each of the forms listed above. A rotary-wing UAV, for example, has a stronger and simpler con-roll and is able to carry a heavier payload compared to the form of fixed-wing. A fixed-wing UAV, on the other hand, has an effective and simpler architecture that enables maintenance processes and is also distinguished by a longer time of flight and greater coverage. Finally, a third form (hybrid-wing) is present, merging the previous ones [11]. In particular, this model has off-and-landing rotors, but it also has fixed wings used for covering wide areas.

Table 1 lists some of the precision farming applications using UAVs. More explicitly, this table presents several types of UAV used in precision farming applications, as well as the type of sensors deployed for each application in terms of payload, altitude and endurance and the related UAV requirements.

Compared to conventional manned aircraft, UAVs can be ef- fectively used for small crop fields at low altitudes with higher precision and low cost. The use of crop management UAVs will provide reliable and real-time data on specific locations. Additionally, crops with high quality images may be provided by UAVs to provide assistance in management of crops, such as disease discovery, tracking agriculture processes, identification of variability caused by the reaction of crops to irrigation, management of weeds and reduction of herbicide levels [16,19],. A comparison between UAVs, conventional manned aircraft and satellite-based systems is provided in Fig. 7. in terms of system cost, endurance, availability, deployment time, area of coverage, weather and working conditions, operational sophistication, use of applications and some examples from the literature are also presented.

2.2. Application of UAVs in precision agriculture

20 UAV applications relevant to the agricultural domain are discussed and analysed in this section. More specifically, these technologies are classified into three categories: a) UAV- based applications for tracking, b) UAV-based applications for spraying, and c) Multi-UAV applications. Table 2 provides a comprehensive summary of the various applications of UAVs in precision agriculture.

Table 1
types of UAVs and their applications in precision agriculture.

Type of UAV	Application	Payload/ Altitude/ Endurance	Type of Sensor Used
Fixed-Wing UAV [12]	Identification of variance in crop response to irrigation	Small camera/ 90 m/ less than 1 h	Thermal Infrared imaging sensor, Thermal Camera
Fieldcopter UAV [13]	Acquisition of high resolution images, assess status of water in vineyard	less than 1 kg/ Low Altitude Platform/ Not Available	Multispectral and thermal cameras
Multi-rotor micro UAV [14]	Supervision of agriculture, identification of disease in citrus	less than 1 kg/ 100 m/ 10 to 20 mins	6-channel multispectral camera, Multi-band imaging sensor.
Mutli-rotor Hexacopter ESAFLY A2500-WH [15]	Investigation of cultivation, multi-spectral data processing to extract VIs	Up to 2.5 kg/ Low Altitude Platform / 12 to 20 mins	Tetracam camera
RC model fixed-wing airframe [16]	Attribute assessment of a grain crop	less than 1 kg/ Low Altitude Platform /	less than 1 hr Digital camera with image sensor.
Vario XLC helicopter [17]	Management of weed, reduction in herbicide use	7 kg/ Low Altitude Platform / 30 min	3D and multispectral imaging vision sensors.
Vector-P UAV [18]	Management of crops such as winter wheat	less than 1 kg/ 105 m to 210 m/ 1 to 6 hrs depending on the payload	Digital colour infrared camera with a red light blocking filter.
Yamaha Aero Robot R-50 [19]	Agriculture montoring	20 kg/ Low Altitude Platform / 1 hr	Azimuth and Differential Global Positioning System (DGPS) sensor system.
Yamaha KG-135, YH300 and AYH3 [16]	Spraying pesticides	22.7 kg/ 1500 m/ 5 hrs	Spraying system equipped with GPS.

1) *UAV-Based monitoring applications:* Crops are tracked by UAV applications thereby providing imaging data that undergoes subsequent processing for the extraction of relevant suitable information and vegetation indices. This leads to the identification of problem areas in a crop suffering from different pests and illnesses. The data that UAV sensors obtain can be spectral, spatial and temporal. Selecting the right sensor and data depends on the design of the appli- cation. Thermal data, for example, is ideal for water status identification, while spectral information is a good choice for the identification of potential plant diseases. Different types of sensors are used in the papers studied, such as thermal, multispectral and hyper spectral cameras. In Fig. 5., some of the most common sensors used have been displayed.
2) *UAV-Based spraying systems:* Some UAV systems are dedicated to applications for spraying. In particular, most of the papers reviewed identify applications capable of spraying sufficient and precise quantities of pesticides and fertilis- ers. These agrochemical commodities are used to improve crop efficiency and to mitigate potential plant diseases and pests. However, their widespread use can produce numerous problems in the human world, such as environmental mental disasters and human diseases such as cancer, neurological disorders and respiratory system complications [20]. Most of the examined papers mount a spraying system and take into account various factors, such as the weather status, that can impact this operation.
3) *Multi-UAV applications:* For PA activities, multi-UAV applications consist of several UAVs. Most of the current works in the literature currently typically concentrate on a single UAV that performs a monitoring operation. However, in some situations, such as large crops, the monitoring process cannot be completed by a single UAV because it is charac- terised by limited energy resources (limited batteries). On the other hand, by dividing the region into several sub-areas based on the number of UAVs [21], this issue can be solved by a multi-UAV programme. It is notable that there is a shortage of papers discussing multi-UAV applications in the literature.

2.3. Deep reinforcement learning techniques in UAVs and applications and energy harvesting techniques used in UAVs

The major problem the UAVs face is energy consumption. UAVs are

Table 2
summary of various applications of UAVs in precision agriculture.

Research Work	Goal	Function	Architecture and Type of UAV	Characteristics	Crop
[22]	Identification of drainage conduits	Observation Procedure	Single Fixed-Wing UAV	NIR Camera,VIS Camera,Thermal Camera	Soybean, Corn.
[23]	Furnished a compound UAV system for airborne imaging	Observation Procedure	Multiple Rotary-Wing UAVs	Hummingbird:pressure sensor, compass, GPS system. AR100: 3- axis gyroscope, magnetometer,Barometer	Vineyard.
[24]	Tracking status of vegetation	Observation Procedure	Single Rotary-Wing UAV	LiDAR, GNSS, Multispectral camera	Winter wheat.
[25]	Sprinkling trees and fruits	Spraying Procedure	Single Rotary-Wing UAV	Spraying Device, Magnetometer, IMU, Barometer, Multispectral camera	Any crop.
[3]	UAV system optimizes the process of spraying by considering weather conditions	Spraying Procedure	Single UAV	Not recognized	Any crop.
[26]	Provided a system for managing and controlling various agricultural UAVs efficiently	Observation Procedure	Mutltiple UAVs in a simulated environment	Not recognized	Any crop.
[27]	Estimationvegetation of status of stress and water	Observation Procedure	Single Rotary-Wing UAV	Thermal camera, Stabilization mechanism, Mul- tispectral camera, GPS system	Pomegranate.
[28]	Enhancement of process of spraying	Spraying Procedure	Multiple Rotary-Wing UAVs	Spraying device	Any crop.
[29]	Tracking status of vegetation	Observation Procedure	Single Rotary-Wing UAV	Multispectral camera, FlightCTRL, GPS system, GSM modem, NaviCtTRL	Vineyard.
[30]	Enhancement of the image acquirement system of UAV	Observation Procedure	Single Fixed-Wing UAV	Multispectral camera, Storing device, Singleboard computer	Potato, Asparagus, Grapes, Sugarcane.

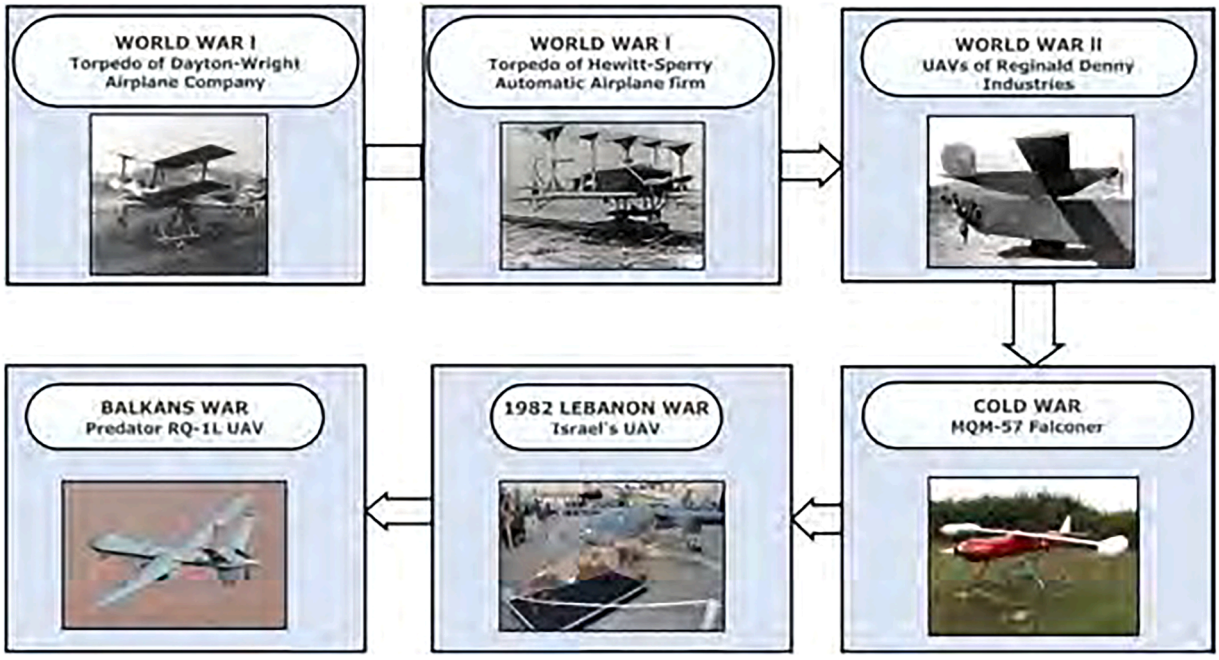

Fig. 5. History of Unmanned Aerial Vehicles across different wars.

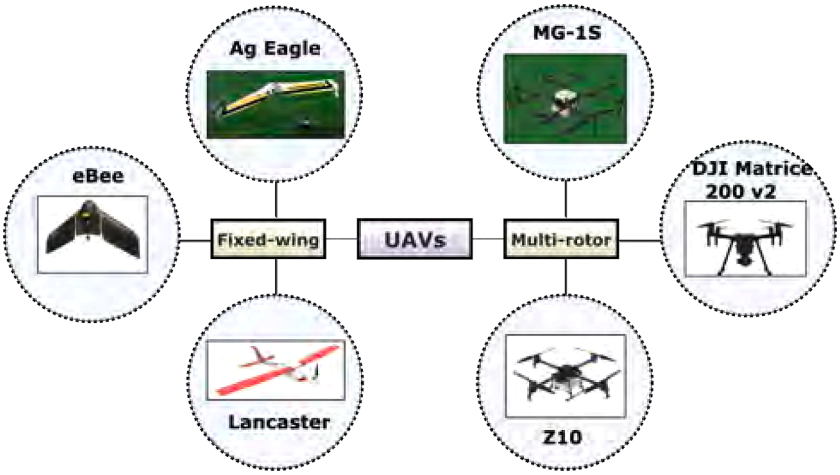

Fig. 6. Types of Unmanned Aerial Vehicles.

most often assisted by the availability of fixed source of energy used for information gathering, propulsion, processing, and distribution of UAVs. In particular, in situations where IoT, WSNs, and special scenarios (such as floods, earthquakes, and similar natural calamities) need to be controlled by UAVs, reducing consumption of energy of the UAVs and the sensors deployed,and extending network life is fundamentally important. We address different notable methods of energy harvesting techniques that can extend airborne times of UAVs and boost its aerial efficiency as well as durability (communication and transportation) in the following sections. We will also address the relevance of deep reinforcement learning (RL) techniques in the implementation of UAVs. An important role is played by deep RL techniques in finding the solution of challenging problems with the help of UAVs, such as UAV trajectory optimization, energy saving and mobile platform landing etc. Table 3 gives a brief description of the mentioned techniques of DRL and energy harvesting.

1) *Energy Harvesting Techniques:* The energy potential of UAVs is a crucial factor in the achievement of any task. Enlarging the battery size or providing UAVs with additional energy resources, the payload increases and absorbs more energy and becomes a crucial problem in the operation of UAVs. The researchers put forward the following directions or suggestions mitigate the issue of UAV battery power energy restriction.

Battery Management: Literature related to battery management suggests the charging of the batteries properly and their proper scheduled replacement for achieving the goal. A model using the particle philtre algorithm was built in [51] to help in predicting the time taken to charge a battery on the basis on UAVs. Authors also discussed core duty of battery and its scheduling for the UAVs in [52].

The goal is minimising the battery degradation rate in the UAVs. They presented an autonomous battery swapping concept in [53]. Following this paper, several researchers [54] advanced this concept of switching batteries. The UAV is connected with an external power supply during the swapping process to make sure UAV functions smoothly as well as avoid the loss of UAV data. To continue the mission ahead, the rechargeable depleted battery of the UAV is exchanged by a

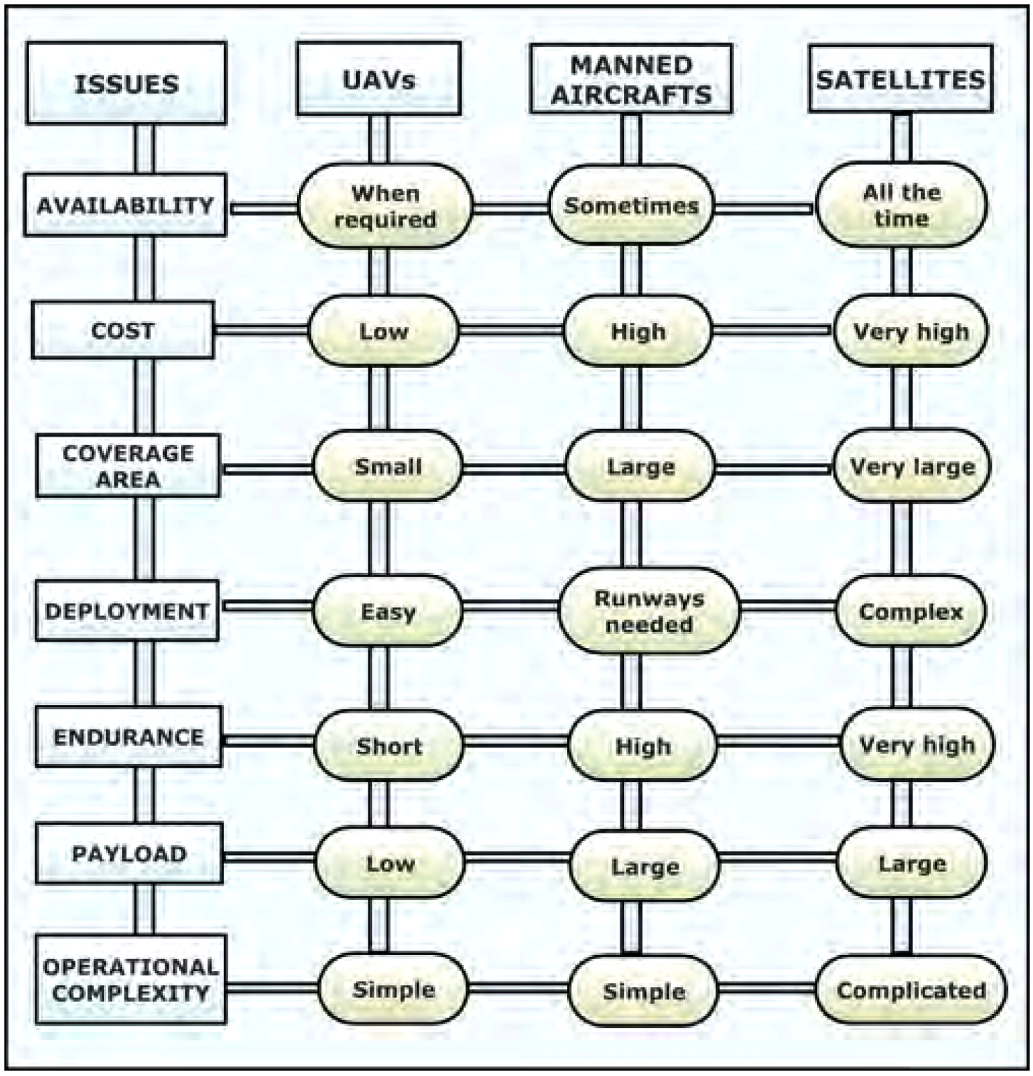

Fig. 7. A comparison between UAVs, manned aircrafts and satellites based on various parameters.

completely charged battery.

Wireless Charging: A new idea is UAV battery charging through wireless power transfer, and the research to make it feasible is going on throughout the world. The principle of recharging the UAVs directly from the power lines is explored in [48], and the subsequent results of their experiment indicate positive change. In [47], the authors probe into an automated UAV charging system in which recharge points centred on solar energy are developed along the flying tra- jectory of UAVs. Authors used magnetic resonance-dependent techniques to help in recharging the UAV batteries in [49] and the wireless power transmission method established on the basis of recharging micro-UAVs is suggested in [55]. A wireless power transfer principle based on capacitive coupling technology is suggested in [50] for recharging UAVs.

Solar Energy: UAVs based on solar energy are the perfect option when the UAV needs to be in the air at high altitudes for a longer periods. Power consumption based on solar energy is used by these UAVs at daytime, though a fixed battery is also used as a subaltern resource sometimes such as at night and in unfavourable weather. Advancements in solar cell technology, improvement of long-range UAV flight endurance, cost-effectiveness and its environmentally friendly design make UAVs based on solar energy, the most desirable option. The authors demonstrated the flights of UAVs based on solar energy in [46] stayed in the air for roughly twenty- eight hours. In [56], the authors developed a UAV model based on solar energy and verified it under various conditions of the weather. The results of their experiment indicate that a solar cell's productions are significantly influenced by the temperature of the environment. The authors also explored the idea of solar energy-based UAVs in [57] while investigating the effects of changing solar radiance strengths and temperatures at different UAV flights' angles.

Machine Learning and Data Communication Techniques: Communication of data has a major effect on energy uses of UAVs and their flight time. Energy-efficient efficiency will benefit from the use of sophisticated AI-based and machine learning techniques to coordinate multiple energy consuming variables well. In optimising the trajectory of UAVs, data transfers, necessary velocity throughout wireless battery charging, battery scheduling, and other energy efficiency related applications, machine learning and AI-based techniques may play an important role. Additionally, the network layer, data link layer and protocols of the physical layer would be enhanced by the energy-efficient UAV networks for guaranteeing the optimal performance of UAVs during assigned deputations. The authors have contrasted different algorithms in the various layers in [58].

2) *Deep Reinforcement Learning Techniques Used in UAVs:* There are actually numerous problems faced by the LTE and next-generation cellular network-assisted UAVs. In the case of LTE coverage, to support high altitude UAVs and BLoS operations, radio signals are

Table 3
few techniques and algorithms fo DRL and energy harvesting.

Literature Work	Year	Techniques/Algorithms	Summary
[31]	2018	Echo State Network (ESN) based Deep RL	Improvement of UAV trajectories and avoidance of inter-vention in BSs.
[32]	2019	Genetic and Simulated Annealing (SA) algorithms	The maximum number of UAVs required to guarantee 5 G connectivity.
[33]	2019	Deep RL, Temporal Difference Method	Problems and limitations in trajectory optimizing.
[34]	2018	Q-Learning Method	Improvement in airborne UAVs sum rate.
[35]	2018	Deep RL algorithm	Seeking optimal UAV locations that serve as relays.
[36]	2019	RL Algorithm	Joint UAV flight course refinement and scheduling of data alerts from sensor nodes or GTs.
[37]	2019	Gazebo based RL Algorithm	Landing of UAVs on ambulant platforms.
[38]	2019	Deep Learning based Convolutional Neural Network	Phenotypic study of the traits of citrus crops.
[39]	2019	Approximation Technique based on CMAC	Prevention of UAVs crash.
[40]	2019	ESN, Q-Learning	UAVs are designed to provide improved summation by solving the joint optimization issue based on UAV path and power control.
[41]	2019	Deep Neural Network	UAVs are employed to establish connectivity that is secure and omni-directional.
[42]	2015	Exchange of UAVs batteries	Automatic switching techniques can increase the battery life of UAVs.
[43]	2019	Solar Energy	Enhancement in the efficiency of UAVs and aerial endurance.
[44]	2018	Solar Energy	Analyzing the effect of temperature on solar energy and UAV flying time.
[45]	2018	Solar Energy	Effects of temperature on the efficacy UAVs based on solar energy.
[46]	2016	Solar Energy	Enhance in UAVs flying time.
[47]	2016	Solar Energy	Maintaining pads for charging up UAVs throughout flying routes.
[48]	2015	Wireless power charging	Charging up UAVs with wireless power distribution from electric lines.
[49]	2017	Magnetic resonance based recharging technique	UAVs recharge using a approach dependent on magnetic resonance.
[50]	2017	Capacitive coupling	Charging up UAVs using technology based on capacitive coupling.

not universal. The installed BS antennas in LTE are mainly intended to support ground UEs and are down tilted to provide optimum throughput. Similarly, the directional antenna beams are down tilted in the mmWave-assisted 5 G and B5G network architecture to guarantee the optimal data rate at ground UEs. It is impossible to provide omnipresent sky coverage in these types of network architectures to effectively enable all sorts of UAV operations. In addition, because of current antenna architectures, channel path failure models, repeated handovers, existence of operational terrain, extremely non-convex complex optimization issues, etc., UAV-based communication systems have some inadequacy and limitations. Machine learning (ML) and in particular deep reinforcement learning (DRL) protocols can be the best methods to work effectively with certain kinds of complex UAV problems. To recognise the relevance of the application of ML and DRL techniques in issues related to UAVs, we present the most recent literature as follows. Challita et al. in [41], proposed a DRL architecture focused on an ESN to refine trajectories of UAVs. The architecture suggested guarantees data latency and prevention of interruption at GBSs. According to this scheme, UAVs together learn their trajectory, alter transmission power magnitudes and the related association vector. Fadi et al. coined an idea in [32] to use an optimum number of UAVs to provide a cost-effective coverage of the 5 G and B5G network in a given region. For this reason, the authors suggested and demonstrated that the best alter- native was simulated annealing (SA) and genetic algorithms. Zeng et al. [33] studied the numerous problems involved in constructing optimal trajectories for UAVs. They introduced an RL-based trajectory optimization technique using a temporal difference technique to analyse the state value function of the Markov Decision Process (MDP). A Q-learning scheme to boost the amount of various UAVs during operational mode was suggested by Herald et.al [34]. UAVs function as flying BSs in the suggested model and as an intrinsic feature of the network coverage system. The authors in [35] used ESN- based DRL techniques to direct UAVs and minimise GBS interference, while the authors in [59] used radio mapping to define ideal airborne positions for UAVs.

Similarly, from a defence standpoint, diverse efforts are being made to classify airborne UAVs. The authors suggested in [60] the role of k-order Bessel to correctly identify UAVs dependent on rotor numbers, e. g. single rotor or multi-rotor. In [61], Ge at al. used strategies from Random Forest and Intense Learning Machine to determine the quality of soil moisture. There was a use of a collection of training data on the basis of field observation surveys and UAV hyperspectral images by the authors. A joint UAV trajectory optimization architecture and precise timing routine for data updates from GTs were developed by Mohammad et al. [36]. The authors used a protocol for DRL and adequate simulation to obtain meaningful results. In [37], the authors focused on the topic of landing UAVs over a complex surface. They have used the Gazebo-based DRL technique in addition to the Deep Deterministic Policy Gradients (DDPG) algorithm to deal with UAVs landing over the mobile floor. The authors used neural network and image recognition techniques based on DRL in [38] to study the phenotypic characteristics of citrus crops. The collision of UAVs is one of the significant problems when a large number of UAVs travel in a specific region. A DRL-based scheme to maximise the chances of collision with airborne UAVs was suggested by the authors, Qiao et al. [39].

3. Security challenges and their solutions in UAV networks

Over 100 UAV sightings occur within a month, as per a survey by the Federal Aviation Administration (FAA). Due to such an increase in UAV sightings, the worldwide transport organizations have started the creation of regulations and the enforcement of fines on UAVs. This is done to make sure that UAV usage is only constructive. The UAV communication network can be highly stable and with lower latency, and fault tolerance, despite the security vulnerabilities [62]. These features can be accomplished by the use of the fifth generation(5 G) telecommunication network, that has already revolutionised industries, specifically the IoT-based industries, where the key issue are latency, network coverage, energy efficiency, and quality of service (QoS) [63].

While the 5 G network provides many benefits for UAV networks, it also possess its own range of security flaws, such as paging occasions and stingrays. The UAV network with 5G-enabled must therefore be shielded from attacks on the network. Blockchain (BC) is a promising option available having a tremendous potential to solve the above problems [64]. In this section, the meaning and background of BC, 5 G, and UAVs are discussed. We also examine how UAV networks are affected by 5 G

and how BC can be used to secure the UAV networks enabled by 5 G.

3.1. Blockchain technology

It is an extremely revolutionary technology conceived in 2008 by Satoshi Nakamoto by the use and advantages of Bitcoins [65]. It is a sequence of blocks linked by the previous block's hash value and so on. The data such as block header, block index, time stamp, block hash, merkle core, prior block hash, and transactions are stored by a block. In BC, there is centralized jurisdiction, making sure that any member belonging to the BC network checks the transaction. Any transaction is cryptographically labelled in such a type of peer-to-peer (P2P) network and confirmation is done by verifying the transaction with any mining node within the complete network [66]. The mining node has a replica of a full ledger, that has fixed accounts of the transactions among the separate BC parties. Once saved on the BC, no transaction record can be changed here without triggering a difference in all the blocks that came later on the BC [67]. In addition, it facilitates accurate monitoring and tracing of block transac- tions. To guarantee the authenticity of agreements, BC blends the advantages of both P2P and cryptography algorithms [68].

3.2. 5G networks

Beyond the 4 G system, 5 G is the next-gene communi- cation network with multiple novel service capabilities and features, for instance, low latency, 10–100x connected de- vices, ultra-high availability, 100 % coverage capacity, 90 % energy reduction, 1000x bandwidth per unit area, and high reliability [62]. It is the latest generation wireless network with many new infrastructure capabilities and functionality outside the 4 G system, such as ultra-low latency, 10–100x connected smartphones, ultra-high availability, 100 % coverage range, 90 % energy consumption, high reliability, and 1000x per unit area bandwidth. It assists cellular connectivity and also device-to-device (D2D) and operates inside a wireless band having high frequency of 28–60 GHz. In order to get a large amount of bandwidth [69] for users, unlicensed frequencies and Long Term Evolution (LTE) bands are also used. The software defined network, large MIMO, millimetre wave, virtualization, network slicing, and D2D communication [70] are different innovations that can be used to boost 5G's performance specifications. The 5 G networking infrastructure will upgrade vast IoT broadband services [71]. For Internet of Things (IoT) applications, the benefits of 5 G may be helpful. Vertical markets have the ability to explode, encouraging the production of a wide variety of facilities with varying types of protection. In addition, 4 G and 5 G are subject to multiple security attacks, such as sybil attack, spoofing attack, alteration attack, etc.

UAVs come in sizes that differentiate them. In defence or mission-critical applications, large UAVs can be used, whereas small-scale UAVs can make up swarms as well as execute routine chores. It's well adjusted to the Indian industry also. India is the top customer for imported drones, according to a report by the Stockholm International Peace Research Institute (SIPRI). Telecom networks are suitable for facilitating inter- drone connectivity in order to enhance the security and com- petence of the operations carried out by drones. 5 G technology offers improved communication and makes these links further stable for outside the line-of-sight UAV operations. High availability and low latency help to prevent mid-air collisions in the management of drone traffic. Telemetry uploading can allow each UAV to recognize its neighboring UAVs. 5 G telecom networks consist of a very wide range, which leads to the enhancement of the current UAV network potential. This enables the generation of large volume of data from sensors which is to be transmitted from cameras. If a drone is linked to a network, its position can also be monitored [72]. BC is the best choice to deal with security problems in UAVs by way of its numerous characteristics to enhance immutability, transparency, and security. UAVs have to make quick decisions in real time, which has a risk element to it. Moreover, with obstacle avoidance, they have to do proper route preparation. In the case of a single UAV, to establish a safe route, it must interact effectively with the GCS. The UAVs can interact and exchange information to coordinate with other UAVs if they function in a swarm. BC functions as a distributed ledger from which it is possible to transact information in a safe way. The UAVs can thus serve as peers for a BC communication net- work to store checked information, using consensus algorithm, in the case of a UAV swarm. BC protection features will keep communications secure for UAV-to-UAV networks. Thus, for all UAV applications, BC can integrate with the UAV networks to form a stable network. A description of various surveys conducted for UAV networks is given in Table 4, Tables 5 and 6. List of abbreviations for table are provided in Table 15.

We also explain Table 4 as follows. A small-sized seed electric seeder integrated with power drive and optical fiber detection technology was built by X. Jin et al. [87], accounting to high efficiency and precision with the help of real-time monitoring of sowing conditions for various seed sizes. Corbari et al. [88] have proposed the integration of a satellite-driven soil–water balance model and meteorological forecasts to empower precision smart irrigation. The model performance was discussed along with emphasizing on the significance of using constant data to calibrate and validate soil hydrological parameters. Ghafar et al. [89] proposed an affordable agricultural robot for the spraying of fertilizer and pesticide, monitoring of crop, and detection of pest. The autonomous prototype system reduced labor costs, but productivity was slightly less than human workers. A flood detection system founded on the IoT, big data, and a convolutional deep neural network (CDNN) was built at Sairam Institute of Technology. A high accuracy of 93,23 % was achieved by the CDNN algorithm, along with a sensitivity of 91.43 %, a specificity of 91.56 %, a precision value of 92.23 %, a recall value of 90.36 %, and an F-score of 91.28 % with a data set of size 500. The flood detection system had outdone existing methods thereby has potential for further improvement by integrating with IoT devices and advanced algorithms to ensure better flood detection capabilities. Kim et al. [90] highlighted the significance of evaluation of drought effects at the time of the vegetative stages of soybean, pointing towards the probability of using phenotypic traits as selection indicators to facilitate the breeding of drought-resistant soybean cultivars, particularly with the considering of the escalating drought and global warming caused crop damage. B. Allred et al. [90] elaborates UAV missions governing the discovery of probable drainage pipes. Conventionally, it requires the farmers to restore drain lines or construct new ones in order to eradicate efficiently the water from the soil. Additionally, the drainage procedures may contribute to the release of amounts of phosphate (PO4) and nitrate (N03), thus leading to the subsequent environmental hazards. So, it is required to know the location of these drain lines; yet, usually, its non-availability in many areas such as many US states like Ohio, Illinois, Minnesota and Indiana is the concern. M.P. Christiansen et al. [91] proposed a UAV system for nursing the production and health state of agriculture crops. Particularly, in the manuscript they have discussed about winter wheat crops by the utilization of a Light Detection and Ranging (LiDAR) sensor integrated on UAV and then employing textual analysis on that data which is provided by UAV.

3.3. Integration of blockchain and 5 G in uav network

BC requires cryptographic techniques to be fitted with UAVs, which guarantees safe communication. This enables organizations to utilize UAVs which hold essential information such as security, financial, and medical applications. BC is a ground-breaking technology in the UAV industry since UAV communication minimizes security and privacy issues. This increases the presence of BC network UAVs. But because of high latency and low scalability problems, conventional telecommunication networks such as 4 G and LTE-A can impede increased participation. Therefore, low latency, massive connectivity, high reliability,

Table 4
utilization of uavs in the precision agriculture.

Location	Technology Used \Technical Characteristics	Exploration\Objective	Task	Crop Test Bed
St. Petersburg, Russia	IoT, robotics, blockchain technology	Leveraged Smart contracts with FCG, Dynamic Robot coalition	Tracking of food	Dynamic robot coalition
Henan University of Science and Technology, Luoyang, China	Technology of optical fiber detection	Electric seeder for miniature vegetables	Sowing of seeds	Vegetable seed electric seeder
Politecnico di Milano, Milan, Italy	IoT	Intelligent irrigation forecast using satellite data, LANDSAT data		A satellite-driven soil–water balance model
University Tenaga Nasional, Selangor Darul Ehsan, Malaysia	IoT	Robot development for pesticide spraying in agriculture	Irrigation	An agricultural robot
Republic of Korea	Remote sensing, SENTINEL-2 satellite	SENTINEL-2 images for characterizing tree composition	Pesticide spraying	Nil
Sairam Institute of Technology, India	CDNN classifier, ML, DL, deep-learning	Flood detection disaster management system	Energy generation	A flood detection system
Rural Development Administration, LemnaTec, Germany	RGB images, Python	Stress restoration inflicted by drought in early vegetative phases of soyabean crop	Flood detection	Nil
United States of America	1. VIS Camera 2. NIR	Detection of Drainage Pipes	Evaluating drought effects	1. sensefly SA eBee
Flakkebjerg, Denmark	Camera 3. Thermal Camera	Monitoring vegetation state	Process monitoring	2. Parrot SA Sequoia
Central Italy	1. LiDAR 2. Multispectral	Monitoring vegetation state	Process monitoring	3.senseFly SA
Thailand	camera 3. IMU 4. GNSS	Investigation of computational resources at the time of a monitoring process.	Process monitoring	thermoMap
Traibuenas, Navarra, Spain	1. Multispectral camera 2.		Process monitoring	4. emotion3 5. Tipping
Ica, Perú	GPS system 3. FlightCTRL	Evaluation of water stress	Process monitoring	bucket Rain Collector (Spectrum Technologies, Inc.) 6. WaterScout SMEC 300 Soil Moisture/Temperature Sensors (Spectrum Technologies, Inc) 7. Pix4Dmapper Pro-(Pix4D SA)
Florida,USA	4. NaviCtTRL 5. First	Optimization of the image acquisition system of UAV	Process monitoring	1. DJI Matrice 100 UAV 2. TB48D battery pack 3. Odroid XU4 4. Velodyne VLP-16 LiDAR 5. Point Grey Chameleon3 3.2 MP Color camera 6. Sony imx265 sensor 7. Vectornav VN-200 IMU MAXTENA M1227HCT-A2-SMA antenna 8. Trimble BD920 GNSS 9. ROS

Table 5
summary of different existing uav network surveys.

Literature Work	Goal	Advantages	Drawbacks	5GF	BCF	UAVF
[73]	To offer a summary on 5 G network privacy issues and associated networks technology.	Described every security concern and its resolution in a tabulated form.	Not tailored to issues of privacy, Did not discuss BC technology.	Yes	No	No
[74]	To deliver a secure and reliable data dissemination system model.	Evaluates conceived system design with previous works.	Does not give a categorization.	No	Yes	Yes
[75]	To investigate publications which propose solutions for IoT security.	Based on questionnaires, numerous problems in devising IoT security solutions are highlighted and pro- poses how BC can solve them.	Gives just logical Solutions, No lab tests con- ducted.	No	Yes	No
[76]	To assess research on cybersecurity pertaining to UAVs.	Provided a categorization for UAV cyber-attacks.	The study emphasizes on the consequences for small UAVs and not big UAVs.	No	No	Yes
[77]	To analyze current 4 G and 5 G network security and data safety solutions.	Categorisation and compilation of problems and their preventive mea- sures.	No emphasis on problems of availability and credi- bility.	Yes	No	No
[78]	To offer a comprehensive assessment of IoT authen- tication methods.	Explains more than 40 protocols divided into five separate groups.	Just the authentication schemes addressed.	No	No	No
[58]	To review research on numerous topics pertaining to UAV communication networks.	Assesses different aspects of UAV networks, making it exclusive.	Concentrates on routing problems, smooth delivery and energy management.	No	No	Yes

and energy efficiency will be brought to the system by the implementation of 5 G in UAV communication. The consolidation of BC and 5 G has immense promise and therefore should be completely secured in both the commercial and defence sectors particularly in the military applications. Military data may be sensitive or mission-critical information and must therefore be protected from all potential attacks on network [92]. Through the combination of 5 G for networking and, BC for security, UAV connectivity is made highly secure against potential network vulnerabilities.

3.4. UAV network issues

Different network problems have been considered and discussed, such as reliability, fault tolerance, energy efficiency, latency, packet

Table 6
summary of different existing uav network surveys.

Literature Work	Goal	Advantages	Drawbacks	5GF	BCF	UAVF
[79]	To demonstrate how BC can be implemented to solve IoT protection and privacy problems.	BC operating mechanisms stopped stalker miner attack.	BC approaches are not small and lightweight, Just investigated stalker attack.	No	Yes	No
[80]	Assesses the 5 G compliance requirements.	Study of network safety of network architectures.	Emphasis on 5 G.	Yes	No	No
[81]	Investigating if blockchain could be used to combat various cyber attacks.	Broadens the use of UAV swarm networks can to blockchain.	Examines only one system for securing a UAV swarm.	No	Yes	Yes
[82]	Reviewing existing security challenges in IoT as well as how blockchain can resolve them.	Mapping significant problems to resolutions in a tabular format.	Recent developments in 5 G connectivity is not dis- cussed.	No	Yes	No
[83]	To study problems, criteria and solutions relating to UAV.	Primarily emphasised on UAVs and their resilience and confidentiality concerns.	Privacy and security issues are focused on.	No	No	Yes
[84]	Mapping how BC technologies can be utilized to authenticate.	Generates a categorization system for BC network authentication.	Concentrated only on concerns of authentication.	No	Yes	No
[85]	Identify problems on how BC should be extended to IoT and some of the alter- natives suggested.	Based on safety and efficiency concerns, the connectivity issues were not addressed.	Concentrates more broadly on IoT.	No	Yes	No
[86]	It addresses possible advantages and uses of UAVs.	Provides the essence of every section when finished.	No exploration of privacy and security problems.	Yes	No	Yes

overhead, bandwidth, system transparency, and QoS, in this section. The numerous network problems of UAV networks are represented in Fig. 8.

1) *Fault tolerance:* Fault tolerance is a system's feature that allows the system to continue to function even while some nodes of the system are offline [93]. Bozic et al. [94] introduced BC communication network implementations and illustrated the spatial dispersion of BC nodes that can give a leverage against problems with a single fixed location of failure. BC's fault tolerance is proven in this manner that there is no detrimental impact on the network even when a few nodes go offline. Additionally, as the nodes goes online again, they are synchronised with the rest, as though they had never gone offline. In order to protect data privacy and dignity, Rahman et al. [95], introduced an in-home therapy management system with BC-Tor based distributed transactions. BC will remove a middleman's need to add robustness to the implementation of security. The distributed design of BC ensures redundancy, as there are multiple versions of data without a single point loss.
2) *Reliability:* It is the characteristic of a device that indicates that it operates continuously without deterioration according to expectations. It is also regarded, over time, as consistency. Yuan et al. [96] have provided guidelines for developing an incredibly dependable communications system for UAV swarms. To boost the hardware of the communication device, a new LoRa (Long Range) gateway has been developed to support the UAV swarm's local star topology network. The authors reported that the LoRa is an improvement in terms of performance over WiFi. But the durability of 5 G networking technologies was not discussed then. A communication protocol in swarm communication was developed by authors in [97] to make autonomous decisions about their actions. The issue of a security vulnerability is solved by decentralized management through BC. As control is individualized, with minimum risk of the complete swarm

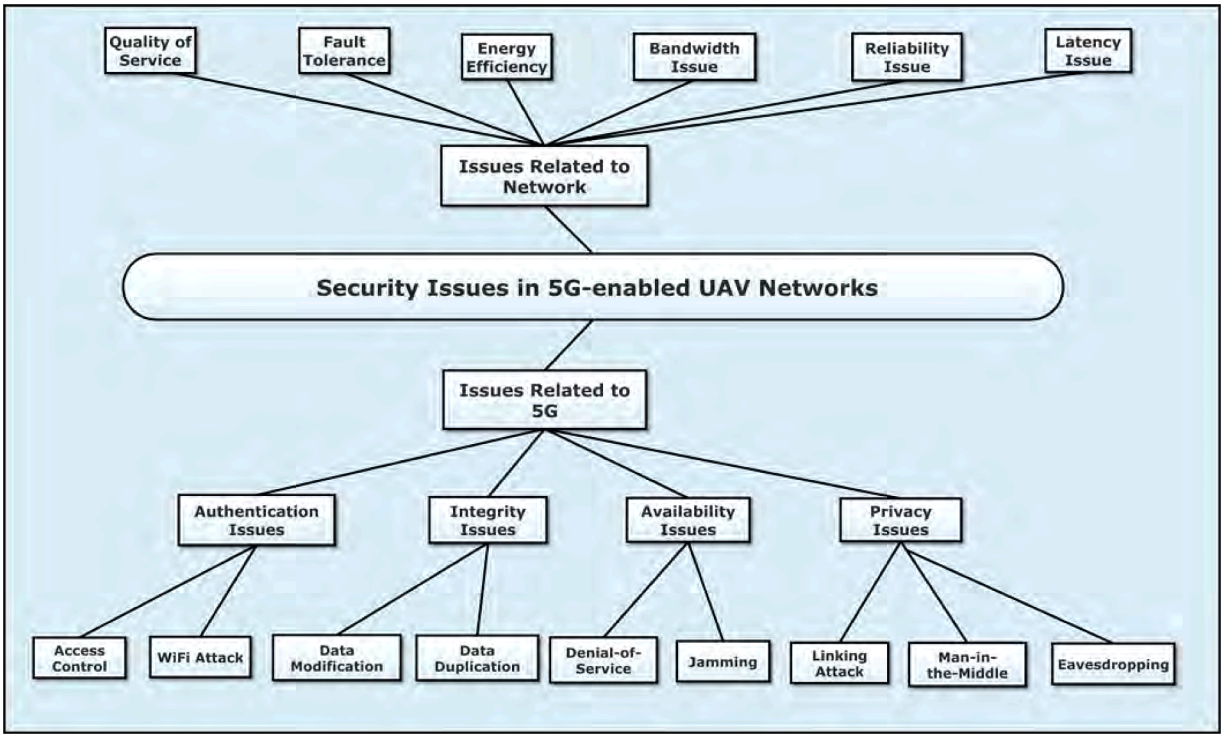

Fig. 8. Common security issues in 5G-enabled UAV networks.

failure, this increases the efficiency of nodes/drones. In [98], the authors suggested a high-level security control system focused on BC technologies for various IoT devices. A machine identification-based key mechanism was utilised to improve the reliability and security of data. A mode was suggested for the credibility and security of the current BC system to be strengthened. To boost the reliability of the data and systems used, they have used MD5, IP verification, and multiplicative inverse. The comparative study of various data integrity, availability and reliability schemes applied to UAV networks is demonstrated in Tables 7 and 8.

3) *Energy efficiency:* In the entire UAV communication network and even for IoT applications, energy efficiency is a key parameter [99]. High energy efficiency decreases both capital and operating spending. 5 G communication guarantees up to 3 days of battery life for mobile and 15 years for IoT devices [100]. Several authors around the world are focusing on accomplishing elevated efficiency of energy. Sharma et al. [101] introduced a head drone system. In this process, as and when the resources of the parent drone shift, the BC's controller/parent/coordinator drone can change easily. This makes the network further energy-efficient and long-lived as it balances the quantity of energy that remains in every drone. For ubiquitous computing that eliminates the requirement for colossus ledgers and long transactions, a master-slave BC system was built in [102]. It is extremely well suited for mobile and IoT devices that consume low-power. Accessibility, efficiency, scalability, and performance have been examined and proven by numerous studies using different mobile devices. Sharma et al. [103] suggested a novel BC-based DMM scheme to solve different security problems with less power consumption. Since it reduces the count of addresses needed to be installed on the mobile nodes (MN), and also because of its single hop communication, as well as related addresses for one switch, it can improve energy efficiency. Dorri et al. [104] purported a lightweight IoT infrastructure design based on BC, which reduces its overheads. To verify transactions, they introduced disseminated trust while cutting down the processing overhead at an individual node. Subsequently, testing on a network of fifty nodes with the NS3 simulator, it was seen that this design reduces processing overhead by fifty percent owing to the mechanism of distributed trust scheme. The comparative analysis proposed by different authors of various energy-efficiency and latency schemes used in the UAV network is shown in Tables 9 and 10.
4) *Latency:* Latency is the period of time from source to destination that a packet has to navigate. Round-trip time is sometimes regarded as network latency. It primarily relies upon the connections employed for the network and the hardware. Grasso et al. [105] demonstrated a tactile architecture based on internet and enabled by 5 G for video surveillance systems. It targets at transmitting collected pictures with the round trip time of just under 1 ms. In order to accomplish this, a microcomputer was set up on every drone by the authors. 5 G software can aid reduce latency too. Wang et al. [106], for example, exhibited an customizable video streaming algorithm for UAVs to minimise the scheme time lag noted in [105]. A system named SkyEyes was developed by the authors to address uncertain wireless connection capabilities and meet requirements for the quality of video. It uses compression of data and video conversion rate on the basis of location sensors and the buffer status of the client to achieve their target. In order to reduce transfer time, this can alter the data size. Through experiments, the authors have found that BC cannot execute on restricted IoT devices reliably.
5) *Authentication:* The method of validating somebody (UAV) who declares himself to be someone, is authentication. It is essential that the UAV network is kept secured and safe from malevolent users [107]. Two-factor or multi-factor authentications are now opted to enhance the security aspects. Attacks on wifi, access control, and fabrication attacks are a few authentication elements to be studied, which are explained as follows [108].

Access control: It only permits authenticated users to access computing resources and utilise them. This mecha- nism prohibits UAV communication networks from controlling UAVs or remote data access by unauthorised or malicious users. Access control can be physical (limited area access) as well as logical (data and connection number controls) [100]. Sharma et al. [101] addressed the use of UAVs for connectivity amongst varied networks to create a impenetrable wireless communication network. BC is also employed by the authors for building trust between UAVs to reduce network response time and costs. To decrease network latency and overheads, BC has been used by them to build trust between UAVs. Public and private keys can ensure the security of network access. A public key helps to identify or authenticate drones, while a private key provides drones the right to use information transmitted from various neighbouring drones.

WiFi attack: In wifi attack, a malevolent user strives to seize command of UAVs by wiretapping their data packets over wifi transmission channels. This is a kind of MIM attack that gets hold of the packets of data and is also able to gain access to the UAV system [109]. The cybersecurity challenges in drone-enabled secured public networks, that can be skyjacked by sensors used in UAVs or cellular signals, have been discussed by He et al. [110]. Key management attribute-based encryption (ABE) and suggested encryption of homomorphic data aggregation are proposed by the authors. This method will safeguard against attacks on WiFi, such as SkyJet.

Table 7
summary of different existing uav network surveys.

Literature Work	Integrity/ Availability/ Reliabil- ity	Goal	Procedure	Technology Used	A/ F	ID	BCF
[115]	Integrity, Availability	To illustrate how safe their smart-home system based on BC is.	Shared key	IoT	Yes	Yes	Yes
[122]	Integrity, Availability	How air traffic management can be implemented with geofencing for UAVs.	Consensus	Geofencing, UAVs	No	No	Yes
[123]	Integrity	To demonstrate how BC can be employed to preserve an IoT device's au- thentication of the data to use.	To verify the credibility of obtained knowledge, con- sult the impervious BC	SCs, Ethereum, Ubuntu	Yes	Yes	Yes
[124]	Integrity, Availability	BC to address problems of anonymity in 5 G content- centric networks.	Local caching	Content Centric Networking, 5G	Yes	Yes	Yes
[111]	Integrity, Availability	Employ BC to construct IoT framework.	RSA public key cryptosystem and private keys	Ethereum, IoT	Yes	Yes	Yes
[125]	Integrity	To suggest IoT data capture scheme based on blockchain.	Merkle Tree	IoT, Edge Computing	Yes	Yes	Yes
[97]	Integrity, Reliability	Technique for arranging the protocol of communication amongst repre- sentatives of a decision-making system.	Cryptographic keys created locally	Ethereum, SCs	Yes	Yes	Yes

Table 8
summary of different existing uav network surveys.

Literature Work	Integrity/ Availability/ Reliabil- ity	Goal	Procedure	Technology Used	A/ F	ID	BCF
[126]	Integrity	To collect data securely using drones and commu- nicate with BC.	Migrating the processing of data to the cloud	Chainpoint, Apache, Ubuntu	Yes	Yes	Yes
[102]	Integrity	Possible new BC framework for ubiquitous com- putation.	Encryption of data, management of key,	Master-Slave, Bitcoinplatform	Yes	Yes	Yes
[97]	Integrity, Reliability	Presents a management system for in-home treat- ment using IoT and BC.	BC, Tor	Edge Computing, IoT, Tor	Yes	Yes	Yes
[101]	Integrity	Drones secured via BC are used as inter-service sup- plier nodes.	Private and public keys	NA	Yes	No	Yes
[127]	Integrity, Availability	To introduce a secure design of the dam surveil- lance system based on blockchain.	Data anchoring, Permanent Proof	UAV broker, sensor cloud, UAV cloud, Bitcoin	Yes	Yes	Yes
[128]	Availability	To recommend a lightweight structure for BC that preserves much of its advantages.	Clusters and public keys	IoT, BC Network	Yes	Yes	Yes
[129]	Availability, Reliability	Presenting a new super reliable drone-caching scheme based on blockchain.	Drones used as caching servers when required	Tor, Mobile Edge Computing, IoT	Yes	Yes	Yes

Table 9
an analysis of various energy efficiency and latency schemes used in uav networks.

Literature Work	Goal	Procedure	Technology Used	A/ F	ID	BCF
[104]	Advocated a lightweight structure centered on BC for IoT.	BC, Smart Contracts (SC)	Immutable Ledger, Cloud Storage, Smart Home Manager, NS3 simulator	Yes	Yes	Yes
[126]	Secured data gathering and communication by	BC using drone.	Transfering the storing and management of data to the cloud. Ubuntu, Chain point, Apache	Yes	Yes	Yes
[130]	Applying BC and SC to mobile adhoc networks.	POS and decentralized BFT	SCs	No	No	Yes
[102]	Potential new BC framework for ubiquitous computation.	Nodes as master and slaves	Bitcoin programme, Master-Slave	Yes	Yes	Yes
[103]	Proposition for a stable BC based DMM schema.	Communication in a hop	DMM, Fog Networks, SDN	No	Yes	Yes
[101]	Drones secured using BC are utilized as inter-service supplier nodes.	As power declines, the coordinator drone reconfig- ures	NA	Yes	No	Yes
[131]	Postulated an iterative algorithm, that optimise every other varying block in UAV.	Dinkelbach's algorithm	DF protocol for transmission	No	Yes	No

Table 10
an analysis of various energy efficiency and latency schemes used in uav networks.

Literature Work	Goal	Procedure	Technology Used	A/ F	ID	BCF
[122]	How UAVs can be operated in air traffic utilizing geofencing.	Consensus	UAVs, Geofencing,	No	Yes	Yes
[128]	To suggest a BC lightweight system that preserves the majority of its advantages.	Beta Reputation System, Diffie Hellman algorithm	Overlay BC Network, IoT	Yes	Yes	Yes
[105]	To formulate video monitoring solutions with a responsive internet framework.	Process information on the video capture software itself	Markov chains, Tactile Internet Network, Micro- computer on each drone	Yes	Yes	No
[132]	The analysis of protocols of distributed ledger is done from an IoT perspective.	Grouping of off and on chain protocols	Ethereum, SCs, Hyper-ledger	Yes	No	Yes
[97]	A therapy network based on BC and Edge Computing.	Mechanism of consensus by adopting longest chain law	IoT, Tor-BC, MEC	Yes	Yes	Yes
[133]	To create a low latency UAV communication system.	Distributed Antenna system	NA	Yes	Yes	No
[106]	UAV-adaptive streaming services prototype.	Adaptation of content encoding and video-rate for viewing	DASH video format, Drones	Yes	Yes	No

Fabrication: Fabrication is also referred to as forging and exploited by mimicking information to get around verification checks. It is also employed for accessing or adding new data/service information. Huh et al. [111] introduced a platform using BC technology for various IoT applications. The authors used the RSA algorithm in which stores the public keys in a BC and individual devices have private keys. They also argued that algorithms of consensus can also act as an obstruction against counterfeit attacks. It is possible to classify fabrication attacks as message forgery attacks and UAV spoofing attacks.

6) *Privacy:* This segment addresses state-of-the-art mecha- nisms to restrict access to legitimate information by unautho- rised users, which is also known as confidentiality [112]. A comparative overview of various authentication and privacy mechanisms employed in UAV communication networks is given in Tables 11 and 12.

Anonymity and location privacy: Anonymity, while ac- cessing the web, is to avoid tracing one's own identity. It also avoids surveillance of networks and analysis of traffic. To retain anonymity, many freeware applications, for example, Tor and freenet, are available. Yang et al. [113], with an anonymous access recognition approach, tackled the problem of secured admission while maintaining small network costs. In this approach, by consensus between chosen parties, trusted recognition is carried out. To maintain secrecy, a public key authenticated based on the originating location is created.

Table 11
comparison of different data authentication and privacy schemes used in uav networks.

Literature Work	Authentication/ Privacy	Goal	Procedure	Technology Used	A/ F	ID	BCF
[134]	Authentication	Utilizing BC to deliver an inno- vative EMR system.	SCs, mechanism like DNS	Ethereum, SCs	No	Yes	Yes
[135]	Authentication	Find out the ways in which BC can improve perseverance ofairborne networks.	BC and crypto-graphic keys	BC, cryptography	No	No	No
[135]	Authentication	Proposing a device concept with an Ethereum blockchain for drone protection communication.	Keys for encrytion and decryp- tion	Internet of Drones (IoD), Ethereum	Yes	Yes	Yes
[136]	Authentication	Advocate a BC-based lightweight architecture for IoT.	Multisig and genesis transactions	Immutable Ledger, Cloud Storage, Smart Home Manager	Yes	Yes	Yes
–	Both	To suggest a BC lightweight system that preserves the majority of its advantages.	Beta Reputation System, Diffie Hellman algorithm	Overlay BC Network, IoT	Yes	Yes	Yes
[137]	Both	How and when to apply BC to swarm robotics.	Digital signature cryptography	Drones	No	No	Yes

Table 12
comparison of different data authentication and privacy schemes used in UAV networks.

LiteratureWork	Authentication/ Privacy	Goal	Procedure	Technology Used	A/ F	ID	BCF
[138]	Authentication	BC to fix privacy challenges in data centric 5 G networks.	Symmetric key algorithm	5 G, Data Centric Networking	Yes	Yes	Yes
[139]	Authentication	Review of concerns regarding drone cybersecurity.	Homomorphic encryption	Drones	No	No	No
[140]	Authentication	Employ BC to construct IoT framework.	RSA, consensus algorithm	Ethereum, IoT	Yes	Yes	Yes
–	Authentication	Process for arranging the protocol of communication among representatives of a decision- making system.	Cryptographic keys created locally	Ethereum, SCs	Yes	Yes	Yes
–	Authentication	Probable modern BC framework for ubiquitous computing.	Encryption of content, Management of key	Bitcoin system, Master-Slave	Yes	Yes	Yes
[141]	Authentication	Presents technologies to guarantee that autonomous vehicles are cyber-secure.	BC and private keys	5 G network slicing, Data Centric Networking	Yes	No	Yes

The data can be encrypted and accessed to preserve privacy. Using zero information evidence and congruential technique, writers have checked their privacy and secrecy methodology. In [114], the authors suggested a framework based on BC to easily and safely transfer UAV traffic data. BC guarantees protection for data transfer and renders the network robust to line-of-sight blocking.

Linking attack: In this attack, several transactions with the same key are connected by an attacker to locate a neighbouring user's ID. The security review of their proposed BC-based smart home platform was provided by Dorri et al. [115]. This system used a specific key for each computer information for its ledgers to preserve anonymity and avoid linking assault. They tried it out using the Cooja simulator and stated that there was very little improvement in overhead time (20 ms and energy in their proposed system (0.07 mj).

Sybil attack: In P2P communication networks, it is a well- known attack in which every node utilises multiple identities simultaneously to weaken the system's repute for trust. The primary objective of this attack is to achieve full leverage in the communication network to carry out illicit acts either directly or indirectly. A few instances of sybil attack are: numerous false accounts with identical name, BC's 51 percent attack, and several false e-commerce platform ratings of a single identity. To show the legitimacy and credibility of the block to be inserted into the BC network, BC uses the consensus algorithm (proof of work). Both miner nodes are checked for transactions in BC and denied if a flawed transaction occurs [116]. The other ways in which sybil attacks can be stopped are: (i) assigning separate abilities to every participant and (ii) generating identification costs .

Man in the middle attack: An assailant tracks or adjusts the communication amongst the various groups in this attack. An assailant can transfer fake data or falsify an interchange among the UAVs using this method of attack. It can also be used between the UAV and its ground station to send false instructions. Garcia-Magarino et al. [117] suggested a strategy based on BC to preserve UAV network security by corrobo- rating information from various sources about incidents. Here a malicious UAV may be the intruder. This strategy tracks the actions and circumstances of UAVs, such as unlawful border crossings. Additionally, secure asymmetric cryptography is used along with an already shared listing of suitable UAVs for diminishing the MIM threat. An architecture based on BC to ascertain permission and anonymity of cellular networks was introduced by Kiyomoto et al. [118]. In this architecture, service data is maintained in the BC to assure the identity, confidentiality and non-repudiation of records.

Eavesdropping: An intruder secretly listens to the exchange among the different groups in this attack. It is recognized for snooping or sniffing attacks too and is a dormant type of MIM attack that does not intervene with any transmission in the network [119]. An attacker exploits the lax communication channels employed for transmission of data and its reception [120]. A privacy-upholding device devoid of the coupling of 5 G smart grid slices and automotive networks was suggested by Zhang et al. [121]. Two hidden keys, Hash-Homomorphic technique, and Paillier Cryptosystem are used in this solution to ensure stable and protected vehicle- to-vehicle communication. It can be tailored to accommodate UAV communication networks.

4. Security and privacy in smart farming

Per year, 10,420,000 people suffer from diet-related dis- eases, according to the World Health Organisation, and six hundred million people become sick due to consumption of contaminated food that could be infected with germs like bac- teria and viruses, or other contaminants and chemicals. This figure can be massively multiplied by a cyber assault on this food industry aimed at agricultural lands, transport networks, and industrial control systems (ICSs) for food production. The need for resilient infrastructure has been recognised and their defences have been hardened by other essential sectors such as oil, finance or healthcare. The food and agriculture sector, however, remains a low hanging fruit for actors at risk. The University of Minnesota Food Security and Defense

Institute (FPDI) has found that ICSs in the food industry could be distinctly prone to cyberattacks. Cyber assaults on smart farming systems can have significant effects for many players in the environment, if not constantly controlled.

These categories include producers, end-users, food processing companies, cooperatives of agriculture, cattle, government departments, and agriculture-critically dependent countries. Extensive research is now possible on protected IoT devices, smart vehicles, drones, edge cloud, wireless networking and could be applied to the environment of smart farming. How- ever, research on these innovations is done much of the time without taking into account the environment in which they are used. The environmental factors affect complex, smart farming ecosystems, like farm machinery, labour sharing, along with organizational resolutions. The problems specific to this domain like user ability set, location, insider attacks, data generated, require protection mechanisms specific to smart farming. Therefore, before smart farm technology is widely adopted, it demands further research. In the field of smart farming, Fig. 9. summarizes the different security and privacy problems and challenges.

4.1. Categorisation of cyber attacks

In this following section, we describe potential cyber threats in the ecosystem of smart farming. As seen in Fig. 10., we have categorised attacks into four distinct groups. We addressed the attacks specific to information and network domains that can be done on smart farms, inclusive of farming sensors based on IoT. We further investigated supply chain cyber-attacks to illustrate flaws as more and more networks are linked to the internet and confidential data is created.

1) *Data attacks:* There are various types of data attacks as following below. These include:

Insider data leakage: Among other risks, farmers fear the loss of sensitive data since it can be used against them in the grain market. Such data may be leaked by an informant, like a disgruntled employee, to purposely cause damage or sell the sensitive data to rivals. For one, over a span of two years, an ex-employee at Allen and Hoshall still had access to the organization's data. The data obtained

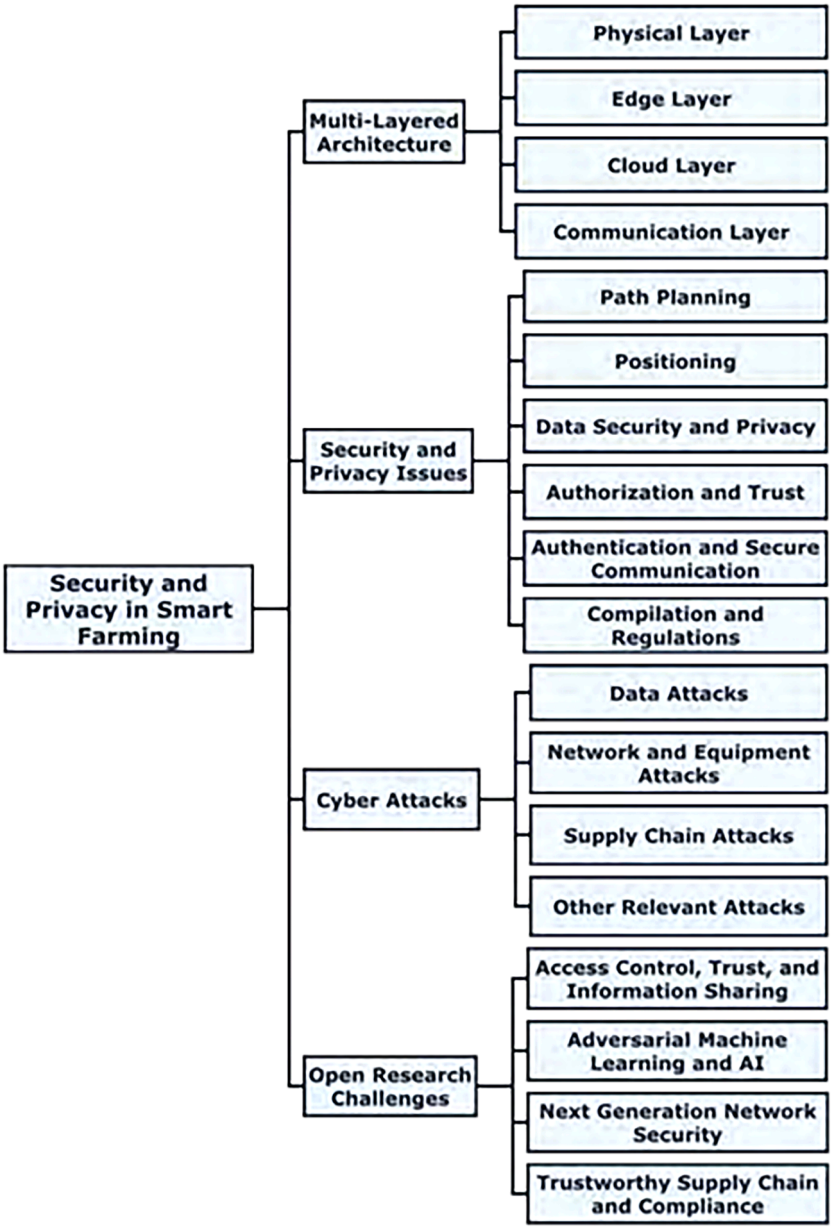

Fig. 9. Various security and privacy issues and challenges in smart farming.

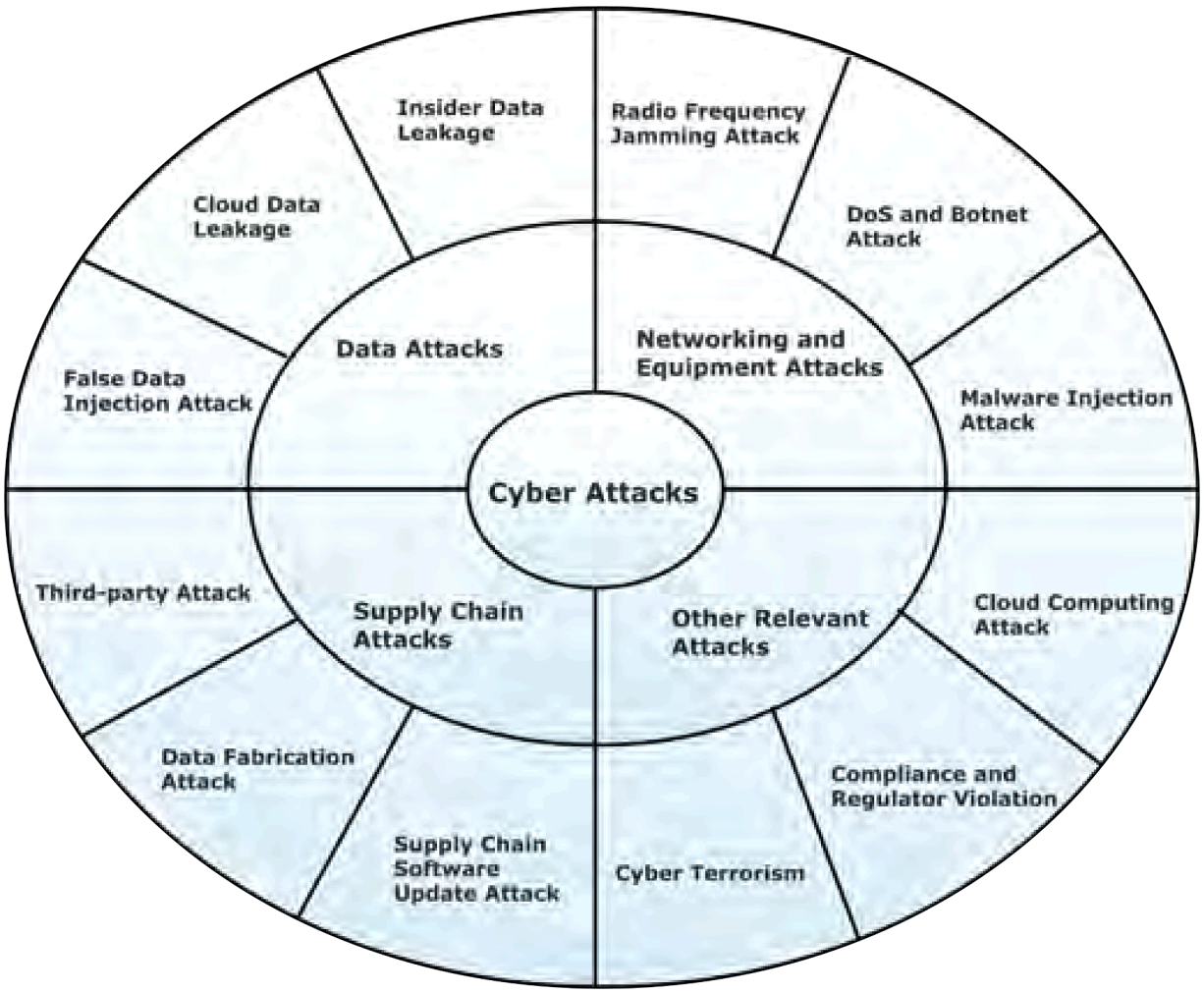

Fig. 10. Various security and privacy issues and challenges in smart farming.

by this employee includes technical schematics, project plans, and marketing information of a total value of five hundred thousand dollars.

Cloud data leakage: Data in Smart farming being highly sensitive can possibly cause the exposure of various proprietary agricultural and economic data from around the world. Cloud data centres are scattered throughout the globe and virtual computers may be installed in data centres situated in various countries in some cases. Data may not be safe when the data is stored in other countries' data centres. Such nations may impose less rigorous security standards on businesses. In addition, under their own countries, the governments of that country can also decrypt or seize data stored on servers. Countries have begun to add regulations for critical data localization for these purposes.

False data injection attack: These are the types of attacks in which the attacker changes or falsifies information that may lead to critical decisions making in real-time, believing that these devices and their implementations are exposed to the adversary. For example, the resulting state could be over-watering, hence, destroying the yield by inserting incorrect information about the level of soil moisture.

Networking and equipment attacks: There are various types of networking and equipment attacks as following below. **Radio frequency (RF) jamming attack:** Smart farm equip- ment, including cellular and satellite networks, also rely on the connectivity of radio frequency. A smart farming device frequently makes use of Global Navigation Satellite Navigation Systems (GNSS) so that the performance can be increased in the goods and methods such as track planning, automatic driving, seeding along with spraying speeds. In order to increase the accuracy of real-time location data, the accomplishment of GNSS is achieved by integrating GPS with Real Time Kinematics (RTK) technology. Through installing several scattered less power consuming jammers to interrupt GNSS in large regions, attackers can jam GNSS for malicious purposes and in turn, keep smart IoT devices from working properly.

Malware injection attack: Malware injection attack [142], where a malware is injected into a linked smart computer by an attacker, is one of the most popular challenges to smart farming. The reason of malware being one of the common threats are that the operation and propagation of it starts immediately through the system in most situations, thereby making it a very tempting target for hackers. Precision farming is widely being embraced, which ensures that a greater number of farmers are using the internet. Many of this type of farm implementations usually use identical device segments (such as usage of LoRa25 or ZigBee26). Hence, other farms with identical installations would most likely be compromised by the same malware that has infected a single smart farm. Malware may steal data on the consumption of agricultural products, information on the procurement of fruit, vegetables and livestock, agricultural machinery data, etc. As part of a botnet that may be used to perform malicious actions operated by an attacker, it can even employ smart devices.

Denial of service attack: Much like what occurred during the 2016 Mirai botnet attack [143], Smart Farming IoT devices can still be exploited to conduct a large-scale distributed denial of service

(DDoS) attacks [144]. An army of dummy CCTVs was abused on that occasion to unleash one of the largest recent DDoS attacks. In a farm with a typically a great number of interconnected network devices and classes in the sense of smart farming, the related types of attacks are more likely. Not only can these attacks interrupt the usual operations of various modules in a single farm, they can also be leveraged to disrupt services in legal cyber related contexts.

Botnet: In the context of IoT, any device can be made to connect to the internet. Various IoT based devices are present at each layer of the architecture in the smart farming ecosystem. These machines can be vulnerable to cyber attacks and a central malicious machine will then monitor them. This network of malicious devices controlled by a single attacker forms an entity called 'Botnet of Things' [145]. An army of corrupted zombie IoT devices [146] could pose a threat across multiple mediums to harm several other networks. Additionally, a smart farm can be made into an Internet of maliciousness instead of Internet of things by cyber attackers. These smart farm systems are usually not designed with protection as a priority; therefore, consumers typically ignore the essential measures of developing effective cybersecurity safety mechanisms.

Supply chain attacks: In a just-in-time setting, the entire agricultural ecosystem and the idea of 'farm to plate' include many organisations working in unison to provide the final customer with quality food. This supply chain system begins with a farm generating raw materials which in turn, are stored as well as processed by all the food businesses [147]. This food after being processed is wrapped and shipped from where the end user orders processed foods to the delivery retailer. It presents possible cybersecurity risks if IoT technology at any point of the food supply chain, as a breach in the security in the just-in-time delivery mechanism might involve a significant cascading impact on the complete food supply chain.

The large-scale attacks such as ransomware WannaCry27, and the latest spate of ransomware in cities all over the United States of America, indicate that just a hack or freezing of data of one interdependent institution is sufficient to destroy a country's entire chain and likely economy.

2) *Other relevant attacks:* There are other different types of attacks also as following below. These include : **Compliance and regulation:** Food processing and farming are heavily regulated entities with various nations having several federal authorities regulating the food manufacturing process. In the USA, the Climate Protection Agency and the Depart- ment of Agriculture impose numerous legislation and business requirements. In the European Union, this role is borne by the Department of Agriculture and Rural Development and related agencies in other countries. In order to guarantee quality food supply, these federal authorities issue enforcement orders. These entities focus entirely on data generated by sensors in the farm with the emergence of smart farming technologies. An attacker targeting a smart farm will particularly insert false information which in turn will affect multiple approval procedures for compliance. If invalidated, this certification process can affect the food supply of a country, affect the price of crops, etc.

Cyber terrorism: The digital embedded infrastructure is being increasingly used in the agriculture sector. This offers terrorists new probabilities to target areas that were historically too far or too hard to hit. Cyber terrorism is a comparatively low-cost industry that has a high potential for payoffs, which makes the threats of agro-terrorism highly dangerous, hence cannot be overlooked. Therefore, it is necessary to pursue solutions that maintain confidence and accountability within the concept of smart farming, furthermore, safeguard the essential resources.

Cloud computing attacks: The cloud is an environment that is very complex, autonomous, heterogeneous and strong. The vast volume of dispersed capital makes it a tough aim for the cloud. However, attackers have used those tools in their favour since the advent of new concepts in cloud applications (such as on-demand applications, auto-scaling, as well as self- provisioning), and in consequence, the cloud has become one of the attacker's most attractive goals. For instance, the advent of cloud auto-scaling has led to a vast portion of cloud-hosted virtual machines being similarly optimised. It is extremely conceivable that all the virtual machines that are auto scaled are also vulnerable if one of the virtual machines is vulnerable. That is because the malware that has infiltrated any one of the virtual machines will easily spread to other virtual machines. The compromised computers may be used as nodes of the global botnets and can therefore be exploited to conduct DoS (DDoS) delivery attacks on a wide scale sufficient to impede cloud functionality.

4.2. Existing research

A multitude of consumer utilities is spawned by the emergence of intelligent devices with connectivity and sensing capabilities, thereby making activities easier and more fruitful for users at the same time. However, the widespread adoption of these gadgets with internet connectivity and data-driven applications across diverse contexts has raised security and privacy concerns, creating these networking systems susceptible to cyber-attacks. Tables 9 and 10 outline state- of-the-art studies, threats and contributions to smart farming with regard to protection and privacy concerns. Based on the focus areas they cover, the current literature has been divided into multiple subsections.

1) *Cyber attacks, threats and proposed solutions:* As more and more producers and cities are embracing agricultural technology, analysts and federal authorities have begun to evaluate the effects of cyber attacks. A report [148] has been issued by the U.S. Department of Homeland Security, which outlines the importance of PA and the resulting vulnerability to cybersecurity and possible vulnerabilities. The study highlights the agricultural information management paradigm of secrecy, honesty, and availability. It describes various PA-related innovations, including in-farm systems, technologies for location and remote sensing, machine learning, etc. It briefly addresses the groups affected by the misuse of agricultural technology, including farmers, livestock growers, and industries that en- courage or depend on agriculture. This article also addresses actual life representations of hypothetical hazard situations. Another promising work [149], highlights the limitations and uncertainties arising from the adoption of precision agriculture technology.

Technology and privacy issues, social engineering, denial of service, cyber-spying agro-terrorism, ransomware, etc. are some of the main challenges discussed. The study also illustrates a security system that helps farmers to better understand the safety consequences of Peer to Peer (P2P) as a network model that uses smart farming contact situations. However, in this form of communication, the system authentication methods depend heavily on public key infrastructure. While the technology is trustworthy, it places needless loads of computing on resource-restricted smart farm IoT devices engaged in safe P2P communication. West [150] built a method to find vulnerabilities in emerging technology and to adapt these technologies to smart farming in a specific way. The platform aim is to measure the degree to which the use of emerging technology in smart farming is vulnerable to cyber-attacks. It utilises the traditional vulnerability scoring system (CVSS) for the evaluation of the threat prediction model. The work highlights the trade-offs in the smart farming world between technological sophistication and adaptation that can contribute to machine compromise. The method in the paper uses three parameters for building a CVSS score: simple parameters, temporal parameters, and environmental parameters. Basic parameters indicate the intrinsicity and magnitude of a vulnerability, while temporal parameters indicate how, due to technological improvements, a vulnerability may alter and affect

the system over time.

2) *Blockchain Related Research:* The utility of blockchain has recently been recognised in realms other than cryptocur- rencies and in financial transactions [151]. Agriculture and food supply chain is one of the areas in which blockchain technology has demonstrated its capability. In [152], the authors therefore review the overall effects, difficulties and op- portunities of current blockchain-based initiatives in the field. Additionally, the sophistication of such projects is objectively examined. The possible hindrances and difficulties that causes obstruction of farmer's acceptability of similar projects and the new cyber-farming systems are discussed. The use of blockchain technologies for food protection was also the subject of Lin et al. [153]. The authors have developed a framework that records and controls the period of food production, including raw material processes, cultivation/breeding, manufacturing, transportation, warehousing and sales. In order to replace manual logging and verification with sensor-based verification, the device often uses different IoT based sensors.

Awan et al. [154] suggested a system for agricultural commodity monitoring life cycle based on IoT and blockchain technologies. To remove the presence of intermediaries or third-party intermediaries and thereby improve legitimacy and confidence, they used smart contracts. Centered on their suggested architecture that included 120 IoT nodes and 20 blockchain manufacturers, the authors introduced a use case. In addition, given various block sizes, they validated their scheme based on its throughput. This work has many pitfalls, however. Too few similar works are included and there is a lack of reference in the literature to other works. In addition, the authors did not provide any knowledge about the essence of the workload used in their studies and neglected to add a baseline benchmark for a fair analysis of the validation results. Table 13 describes the existing solutions on cyber-attacks, features and limitations.

3) *Artificial Intelligence and Machine Learning assisted work:* In addition to promoting the adaptation of applied ana- lytics in smart farming, the introduction of new age advances in artificial intelligence (AI) and machine learning (ML) provides an environment to boost service cybersecurity. The convergence of these technologies helps farmers in intensely competitive markets to obtain higher average yields and greater price control over their goods. Shabadi and Biradar have suggested the design and deployment of a low-cost security monitoring system based on IoT [155]. The device focuses on the physical layer of intelligent farming, where sensor data is obtained. This knowledge is sent to a controller where data is processed to take decisions such as triggering the water sprinkler actuators in the farms. The current work focuses more on the application of smart farming's basic functionalities than on solving protection and privacy concerns. It is quite limited to basic threshold-based decisions, such as triggering the water sprinkler if the soil temperature is above a certain threshold. Another current use of ML in smart farming is real time security control for a remote farm. In circumstances where real-time tracking and alerts are paramount to farming and cybersecurity, AI-supported machine vision programming may process the images detected by a surveillance system. Abuan et al. [156], for example, suggested a neural-based face recognition method that through neural network preparation can be invariant to changes in background light and illumination conditions. Table 14 describes the existing works and models on blockchain, AI and ML in smart farming. It also explains the features and limitations of existing solutions.
4) *Other relevant literature:* An architecture for Precision Agriculture Cybersecurity Approaches was proposed by Chi et al. [157] It tackled the problems of using Wireless Sensor Networks (WSN) in digital virtual farms. They also offer a stable data collection system. Security

Table 13
existing work on cyber attacks and their solutions.

Literature Work	Goal	Features	Drawbacks
[150]	Mainly focuses on exposure of cyber-attack threats in technology (such as sensors, transceivers, and information systems) and in the world of smart agriculture.	A Common Vulnerability Scoring System (CVSS) score is constructed dependent on the technology used in a smart farm, taking into account the climatic aspect of smart agriculture.	In the whole model, CVSS struggles to correctly capture the effect of interactions. Not ideal for extremely diverse networks using diversified protocols and information technologies to reach vulnerability threats.
[158]	Illustrates the essence of the possibility of creating unfamiliar risks in modern technol- ogy.	Emphasizes the scope of the agricultural industry's provision of cyber insurance. Demonstration on the legislative reaction to smart system use and its effect on the protection of smart farms.	Thorough potential technical advice on emerging hazards is lacking. Inadequate claims about potential rules for agriculture and cyber security.
[159]	Increases peer - to - peer (P2P) communications protection in smart farming via a new technology focused on cryptography.	Develops a lightweight process of encryption / decryption to enable a secure P2P messaging solution for smart farming au- thentication.	In comparison with the established technologies, it is not apparent how quick and lightweight the new process is. In a real life situation, the recommended approach has not been thoroughly tested.
[160]	In smart farming, analytical approach is used to illustrate safety threats and obsta- cles.	Examine cybersecurity threats such as social engineering, agro-terrorism, denial of ser- vice malware attacks, and cyber-espionage. Discusses the process for cyber risk control.	No deployment or output. There are no use-cases that represent the orchestration of attacks. Inconsistent differentiation in cyber hazard distinctions from several other fields.
[148]	Recognizes safety risks, hazardous situations and weaknesses in smart cultivation, crops and animals.	Discovers vulnerabilities through the use of information security CIA model. Identi- fies new technologies for PA. Recommends methodologies for security.	Absence of difference between Cyber Physical System (CPS) and PA challenges. *Re*-stricted and complex strategies for cyberse- curity.
[161]	Farmers and agri - business owners are asked regarding their views on cybersecu- rity, and how these expectations can be influenced by age, gender, and education.	Measures rate of past cyber-crime victimi-sation and application of technologies. In- formation about how people respond to es- tablished risks and what encourages them to embrace solutions for defence.	Temporal research can help lead to the comprehension of how views of cyber risks evolve with increased recognition.

(*continued on next page*)

Table 13 (*continued*)

Literature Work	Goal	Features	Drawbacks
[157]	Discuss the complexities of the remote farm's wireless sensor network (WSN) and suggest a security solution system for data transfer in PA.'	A CPS architeture that incorporates the concept of virtual farmlands is proposed. The suggested CPS stream provides increased frequency decision processes in real time. Discuses aspects of the security system.	Conceptual logical structure of a high degree. No models for development or out- comes of review. Incomplete strategies for data security.
[162]	Identifies bioeconomy and explores the security of cyberbioeconomy.	Describes how existing and latest knowledge and technology are used.	No viable approach has been proposed to improve the security of the cyberbioecon- omy.

issues in the agri-food sector were addressed. A summary of emerging technologies in smart farming is given in the paper. In terms of automating agricultural processes, decision making, and forecasts, most smart farms are data driven. The study seeks to increase awareness of the value of cybersecurity in the food and beverage industry.

4.3. Open challenges and research areas

This section addresses open research problems, as shown in Fig. 11., to enhance protection and privacy in the smart farming ecosystem. These open concerns have been separated into four subsections as follows.

1) *Access control, trust and privacy perspective:* Cyber vulnerability issues need to be tackled by the expansion and adaptation of basic studies on current access control, as well as the development of new access control technologies to support complex and adaptive ecosystems in cyber-physical networks such as smart farms. In-farm and cross-farm operations involve permitted coordination between sensors and farmers operating on various farms operating various smart system sets. What kind of operations they may perform must be reviewed, which, depending on the risk factor associated with the procedure, can include single level or multiple level access control? For example, compared with turning on an irrigation system during the rainy season, imagine sowing the field with an autonomous tractor. The delegation and withdrawal of access rights to agricultural activities must be carried out immediately on the basis of a collective arrangement, for example in the case of contingent labour working during the harvesting season. In order to be implemented in such a complex environment, such access control criteria need further study. The definition of trust may also be established when labour that has already worked or equipment borrowed from a 'proven' old friend may have a higher degree of trust relative to machinery and labour recruited from the cooperative sector. In a sharing- dominated CPS domain like smart farming, self-configurable AI assisted smart access control policies need to be developed.
2) *Data perspective:* Smart farming's most notable attribute is its ability to connect between smart devices, which results in an unparalleled amount of data generated [165]. This poses numerous challenges and opens doorways for numerous opportunities for study. Machine learning is an appealing answer for the analysis of big data and the introduction of reliable technologies for defence. Detection of insider data leakage has always been a challenge when consumers have legal access to the device now, making it impossible to track and anticipate such attacks. Several research studies on insider data leakage

Table 14
existing work on the use blockchain, AI and ML in smart farming.

Literature Work	Goal	Features	Drawbacks
[154]	Development of a platform for agricultural commodity monitoring based on blockchain and IoT technologies.	Keeps track of the complete lifecycle of goods using blockchain technique. Create a test bed with 20 blockchain manufacturers and 120 IoT nodes to model a smart farm.	No reference to other literary works. Some details of the modeling of the envisaged system remain vague, including what has been employed to be used for workload and distribution of probability.
[153]	By utilizing blockchain to ensure food traceability improves the overall food safety problems.	Leveraging IoT devices and blockchain technologies helps monitor different facets of the food production cycle. Sensor-based testing of the potential food manufacturing cycle.	For a generic blockchain, the platform is built with particular benefits, given by a unique implementation. There is no stan- dard version. SCs are not enforced on the blockchain.
[163]	Examines blockchain usage above the usual aspects of financial utilization in agriculture.	Offers examples of real life use of companies for agriculture utilizing blockchain. Blockchain is used to establish traceability of food throughout the supply chain.	High-level overview of the applications without any specifics or outcomes of im- plementation.
[152]	Studies the effect of blockchain technologies on the production process of cultivation and food.	The existing blockchain-focused agricultural and food production chain ventures have been critically reviewed.	There are obstacles and difficulties faced byfarmers and farming processes that impede the broader acceptance of blockchain-based ventures.
[164]	Employs ml for smart agriculture security in big data analytics, with a use in the chain of production of milk.	Aims to develop a smart farming computational framework for big data. Operates with two distinct strategies for ML.	The proposed solution was tested in a very small range of use cases and its resilence remains uncertain in a real life situation.
[156]	The implementation of ML for pattern detection of recorded CCTV videos used in farm surveillance is focused.	Protection framework for isolated farms. Surveillance and updates in real time in precision agriculture. Image detection and identification of trends found by smart farm monitoring system.	The solution presented is not modular and scalable. It is not known if it is possible to analyse and interpret different images from numerous cameras parallely in order to fulfil the envisaged system's property of real time.

Table 15
list of abbreviations used in the tables.

Abbreviations	Full form
A/F	Architecture/Framework given
BCF	Blockchain-focused
ID	Implementation done
UAVF	UAV-focused
5GF	5G-focused

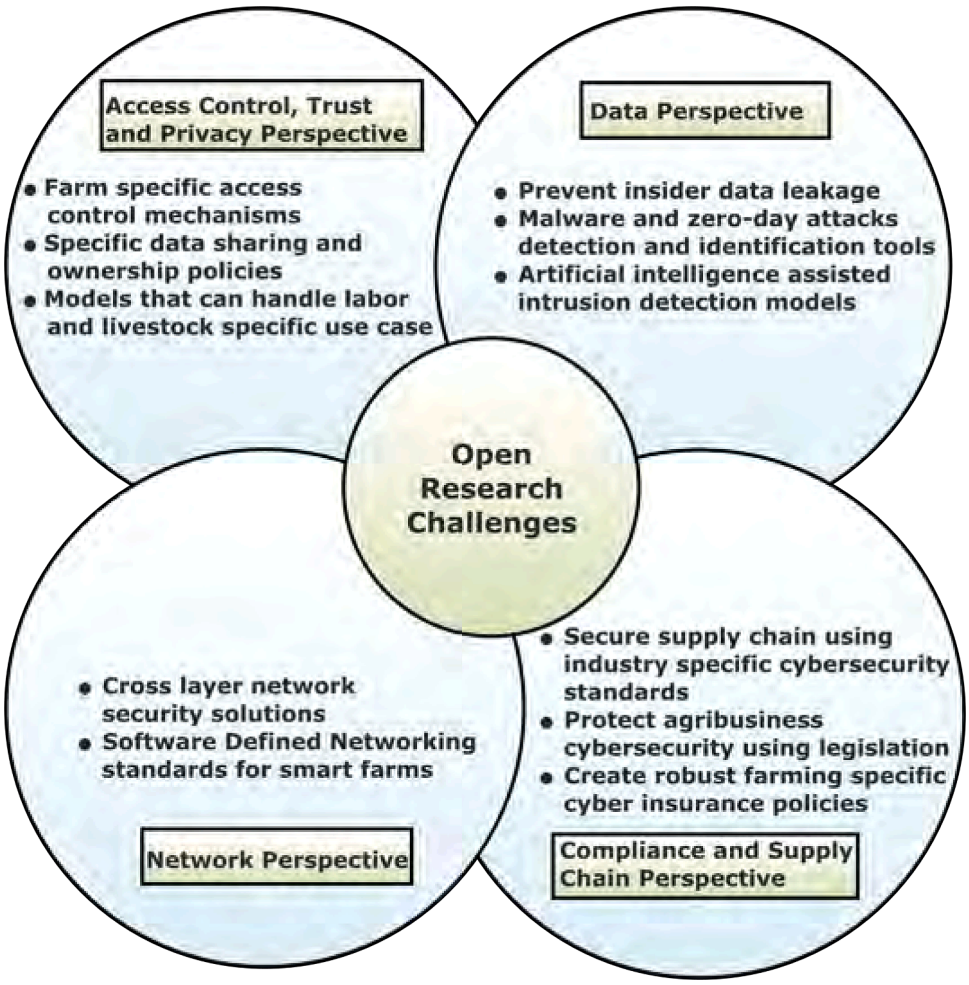

Fig. 11. Open research challenges in cybersecurity of smart farming.

have been done, but none have targeted smart farming environments. In order to understand the likelihood of implementing insider data leakage protection mechanisms in smart farming, more study is required to understand whether specific characteristics of smart farming can help strengthen these mechanisms. Smart farms are highly integrated networks that make it possible for malware to spread through the network to target all interconnected computers.

3) *Network perspective:* Due to some aspects of the un- derlying networking and connectivity systems that are used in the domain, cybersecurity challenges to PA and its equip- ment provide a wide spectrum of risks in security. Next, it is connected to both interactive and physical networking contexts. Many IoT devices are able to operate on the data they obtain from their respective ecosystems in a smart farm system, which abridges the gap betwixt physical and virtual systems. Although it is easier for consumers, it helps cyber-attacks to be more easily translated to physical effects, thereby creating a greater effect. Second, a dynamic connectivity environment is created by devices and levels participating in a PA scheme. Because of the increasing diversity and acces- sibility of IoT products, hyper-connected farming ecosystems exist. In this case, 'complicated' suggests that a multitude of devices operate in an individual smart farm environment in such a way that dynamic communications are possible among them. This intricacy extends an environment's capabilities, but at the expense of a larger assault plane. Several emerging innovations, intelligent farming supports modern networking paragons to counter today's advanced assaults.

One such ambitious networking breakthrough is the Software Defined Network (SDN) [166]. It provides fascinating technological features for network operators by decoupling the control plane from the data plane and providing credit to the programmable network. In nearly all areas of networking, from data centre networks to WANs, wireless, 5 G and recently IoT, this triggers intensive SDN adaptation. Smart farms are proficient to establish an aggregated view of all the linked devices using SDN, beside the way they communicate in an almost real-time way. This holistic perspective strengthens smart farm network resilience, scalability, and manageability, and also endows a big PA network to incorporate effective defence countermeasures against future advanced cyber-attacks. The malleability of SDN and various 5 G next-generation networking technology in the area of smart farming and PA must be further explored.

4) *Compliance and supply chain perspective:* Through the pervasive employment of sensors, autonomous drones, BC, incorporation of AI, numerous agricultural undertakings are dropping back on the security of compliance, legislation and cyber insurance [158]. The whole chain of food supply is in danger due to the evolution of directed malevolent program and other cyber threats.

A hostile attacker directly involved in disrupting the supply chain will threaten different entities and businesses that supply the farms with raw material or process the end user's food. Developing market standards that allow trust between different suppliers of raw materials and downstream food processors is a possible solution to this problem [158]. The creation of these standards, implemented via the

enforcement by national governments, has so far been sluggish. The existent of some cybersecurity standards for numerous smart devices employed in the food supply chain is one example of such a shortcoming. Various laws are being brought in to set minimum standards for operations of internet-connected devices for cybersecurity. In particular situations where separate governments do not want to monitor these encounters, it is dependent on different agricultural firms to defend themselves by calling for best practices in their chain of supply to self-govern cybersecurity. It is possible to push such developments via competitive pressure, market demands, etc.

We talk about various issues that the precision agriculture struggles with, such as resource overuse, uneven tech access, monoculture, intensive animal farming, food safety concerns, inefficient supply chains, environmental damage and resistance to change. These are some challenges that obstruct the efficiency of the farming system and also affects the productivity and sustainability of the ecosystems. However, the industrial revolution (Industry 4.0) brought interconnected AI, big data, IoT, blockchain technologies in one forum and the integration of these technologies into agriculture has shaped "Agriculture 4.0" or "smart farming," thereby, aiming to address the aforementioned challenges. These challenges are well addressed by the technology shift with farmers adopting precision technologies to reduce environmental impact and ensure long-term viability. Resultantly, the smart farming mission is becoming more autonomous and intelligent with the agricultural processes and supply chains automating tasks like planting, seeding, harvesting, and soil sampling. This has also aided in contributing to the efficiency of the farmers reduced labour costs. In this spirit, while conventional precision agriculture faces hurdles, Agriculture 4.0 bids a promising path towards a more sustainable and productive future for smart farming.

5) *Blockchain*: A decentralized database provides exciting possibilities for realizing smart farming in Agriculture 4.0. Its key features lie in its deliverance of attributes like transparency, immutability, and reliability that builds trust amongst the stakeholders in the agricultural supply chain. By eliminating the issues of outmoded corporations, the technology of blockchain facilitates the integration of digital technologies into farming. This integration of disruptive technologies confronts several technical challenges highlighted as follows: -

   a. **Insecure data sharing:** Blockchain's decentralized nature eliminates the need for a single point of failure thereby, making data sharing even more secure.
   b. **Slow satellite detection:** Blockchain can also process data at a faster rate satisfying the in real-time demands, overcoming delays in identifying crop variability.

In addition, the blockchain technology also attends to the anonymity, decentralization and security concerns in smart farming's IoT systems. The agricultural analysts envision a lightweight, distributed farming system that delivers transparent security and caters to the privacy issues. Since the blockchain technology is still in its early stages, it exhibits certain potentials such as: to monitor farm operations securely, improve planning and improve the safety of food. To monitor the farm operations securely, the information can be shared securely across a distributed network, allowing efficient monitoring of irrigation, energy consumption, and labor management. For improved planning, the Blockchain technology helps in the planning of agricultural processes, including tasks for robots, drones, and other autonomous systems. Lastly, for improved food safety, the feature of blockchain's traceability is leveraged in the complex food supply chain addressing information asymmetry. By catering to these challenges, blockchain proves to be more reliable, efficient, and secure for the future of Agriculture 4.0.

5. Conclusion

The UAVs are being employed in numerous civil applica- tions. UAVs are necessary in situations where humans fail to carry out or cannot accomplish dangerous/risky tasks in a timely and effective manner, from peak hour delivery systems to finding inaccessible areas. We have reviewed various applications of UAVs in agriculture such as irrigation, tillage, mapping etc. On-board image processing and in-field analytic capability can be provided by the next generation of UAV sensors, which can provide farmers immediate visibility into the field without the need for cellular access and cloud access. In this paper, alongside their security problems, flaws, and solutions, we have presented comprehensive details on BC infrastructure and UAV communication networks. It provides a discussion and comparison of different recent surveys. UAV security challenges related to 5 G and network vulnerabilities have been categorised and addressed. Various features (such as latency, reliability, and security) are taken from different existing networks, such as 5 G, and introduced in UAV net- works. However even now, in 5G-enabled UAV networks, several problems remain unresolved. To address the above problems, this paper used distributed BC technologies. The paper outlines problems of privacy and security, and underlines the various examples of assaults on smart farms and also on the premises involving the complete food supply chain. This essay then discusses state-of-the-art analysis and recognises valuable work performed in the domain using AI and ML relevant to cyber security. Finally, the paper exemplifies many unresolved problems and research questions relating to the facets of protection and privacy in precision farming. This paper will simulate analysis in order to address data and secu- rity protection problems in the rapidly rising and economically relevant smart farming market.

CRediT authorship contribution statement

Meghna Raj: Methodology, Resources, Writing – original draft. **Harshini N B:** Data curation, Formal analysis, Writing – original draft, Writing – review & editing. **Shashank Gupta:** Conceptualization, Formal analysis, Methodology, Writing – review & editing. **Mohammed Atiquzzaman:** Supervision, Writing – review & editing. **Oshin Rawlley:** Conceptualization, Software, Writing – original draft, Writing – review & editing. **Lavika Goel:** Software, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

This work is supported by I-DAPT HUB FOUNDATION, IIT (BHU), Varanasi for the project ref. no. I-DAPT/IIT (BHU)/2023-24/ Project Sanction/44. dated 19-09-2023.

This work is also supported by CHANAKYA Fellowships of IITI DRISHTI CPS Foundation under the National Mission on Interdisciplinary Cyber-Physical System (NM-ICPS) of the Department of Science and Technology, Government of India. Grant no: CF-2022-PhD-000002.

References

[1] G. Sylvester, *E-agriculture in action: drones for agriculture*. Food and Agriculture Organization ofn the United Nations and International, 2018.
[2] J.V. Stafford, Implementing precision agriculture in the 21st century, J. Agricult. Eng. Res. 76 (3) (2000) 267–275.

[3] S. Hayat, E. Yanmaz, R. Muzaffar, Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint, IEEE Commun. Surveys Tutor. 18 (4) (2016) 2624–2661.
[4] F. Nex, F. Remondino, Uav for 3d mapping applications: a review, Appl. Geomatics 6 (1) (2014) 1–15.
[5] S. Chiesa, M. Fioriti, R. Fusaro, Male uav and its systems as basis of future definitions, Aircraft Eng. Aerospace Techn. (2016).
[6] H. Gonzalez-Jorge, J. Martínez-Sańchez, M. Bueno, et al., Unmanned aerial systems for civil applications: a review, Drones 1 (1) (2017) 2.
[7] J.D. Blom, Unmanned aerial systems: a historical perspective, Cite- seer 45 (2010).
[8] F.M. Mirzaei, S.I. Roumeliotis, A kalman filter-based algorithm for imu-camera calibration: observability analysis and performance evaluation, IEEE Transact. Robot. 24 (5) (2008) 1143–1156.
[9] Y.K. Chan, V. Koo, An introduction to synthetic aperture radar (sar, Progr. Electromagn. Res. B 2 (2008) 27–60.
[10] J.M. Dow, R.E. Neilan, C. Rizos, The international gnss service in a changing landscape of global navigation satellite systems, J. Geod. 83 (3) (2009) 191–198.
[11] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, "Drone technology: types, payloads, applications, frequency spectrum issues and future developments," in *The future of drone use*. Springer, 2016, pp. 21–45.
[12] D. Sullivan, J. Fulton, J. Shaw, G. Bland, Evaluating the sensitivity of an unmanned thermal infrared aerial system to detect water stress in a cotton canopy, Trans. ASABe 50 (6) (2007) 1963–1969.
[13] J. Baluja, M.P. Diago, P. Balda, R. Zorer, F. Meggio, F. Morales, J. Tardaguila, Assessment of vineyard water status variability by thermal and multispectral imagery using an unmanned aerial vehicle (uav, Irrig. Sci. 30 (6) (2012) 511–522.
[14] A.Y. Chen, Y.N. Huang, J.Y. Han, S.C.J. Kang, A review of rotorcraft unmanned aerial vehicle (uav) developments and applications in civil engineering, Smart Struct. Syst 13 (6) (2014) 1065–1094.
[15] S. Candiago, F. Remondino, M. De Giglio, M. Dubbini, M. Gattelli, Evaluating multispectral images and vegetation indices for precision farming applications from uav images, Remote Sens. (Basel) 7 (4) (2015) 4026–4047.
[16] Y. Huang, S.J. Thomson, W.C. Hoffmann, Y. Lan, B.K. Fritz, Development and prospect of unmanned aerial vehicle technologies for agricultural production management, Internat. J. Agricult. Biolog. Eng. 6 (3) (2013) 1–10.
[17] W. Kazmi, M. Bisgaard, F. Garcia-Ruiz, K.D. Hansen, A. la Cour- Harbo, Adaptive surveying and early treatment of crops with a team of autonomous vehicles, in: Proceedings of the 5th European Conference on Mobile Robots ECMR 2011, 2011, pp. 253–258.
[18] E.R. Hunt, W.D. Hively, S.J. Fujikawa, D.S. Linden, C.S. Daughtry, G.W. McCarty, Acquisition of nir-green-blue digital photographs from unmanned aircraft for crop monitoring, Remote Sens. (Basel) 2 (1) (2010) 290–305.
[19] N. Muchiri, S. Kimathi, A review of applications and potential applications of UAV, in: Proceedings of sustainable research and innovation conference, 2016, pp. 280–283.
[20] I. Dhouib, M. Jallouli, A. Annabi, S. Marzouki, N. Gharbi, S. Elfazaa, M. M. Lasram, From immunotoxicity to carcinogenicity: the effects of carbamate pesticides on the immune system, Environ. Sci. Poll. Res. 23 (10) (2016) 9448–9458.
[21] A. Franchi, P.R. Giordano, C. Secchi, H.I. Son, H.H. Bülthoff, A passivity-based decentralized approach for the bilateral teleoperation of a group of uavs with switching topology, in: 2011 IEEE International Conference on Robotics and Automation, IEEE, 2011, pp. 898–905.
[22] B. Allred, N. Eash, R. Freeland, L. Martinez, D. Wishart, Effective and efficient agricultural drainage pipe mapping with uas thermal infrared imagery: a case study, Agric. Water. Manage 197 (2018) 132–137.
[23] A. Barrientos, J. Colorado, J.d. Cerro, A. Martinez, C. Rossi, D. Sanz, J. Valente, Aerial remote sensing in agriculture: a practical approach to area coverage and path planning for fleets of mini aerial robots, J. Field. Robot. 28 (5) (2011) 667–689.
[24] M.P. Christiansen, M.S. Laursen, R.N. Jørgensen, S. Skovsen, R. Gislum, Designing and testing a uav mapping system for agricultural field surveying, Sensors 17 (12) (2017) 2703.
[25] B. Dai, Y. He, F. Gu, L. Yang, J. Han, W. Xu, A vision-based autonomous aerial spray system for precision agriculture, in: 2017 IEEE International Conference on Robotics and Biomimetics (ROBIO), IEEE, 2017, pp. 507–513.
[26] C. Ju, H.I. Son, Multiple uav systems for agricultural applications: control, implementation, and evaluation, Electronics. (Basel) 7 (9) (2018) 162.
[27] P. Katsigiannis, L. Misopolinos, V. Liakopoulos, T.K. Alexandridis, G. Zalidis, An autonomous multi-sensor uav system for reduced- input precision agriculture applications, in: 2016 24th Mediterranean Conference on Control and Automation (MED), IEEE, 2016, pp. 60–64.
[28] M. Daibo, Toroidal vector-potential transformer, in: 2017 Eleventh International Conference on Sensing Technology (ICST)., IEEE, 2017, pp. 1–4.
[29] J. Primicerio, S.F. Di Gennaro, E. Fiorillo, L. Genesio, E. Lugato, A. Matese, F. P. Vaccari, A flexible unmanned aerial vehicle for precision agriculture, Precis. Agric. 13 (4) (2012) 517–523.
[30] J.A. Paredes, J. Gonzalez, C. Saito, A. Flores, Multispectral imaging system with uav integration capabilities for crop analysis, in: 2017 First IEEE International Symposium of Geoscience and Remote Sensing (GRSS-CHILE), IEEE, 2017, pp. 1–4.
[31] U. Challita, W. Saad, C. Bettstetter, Deep reinforcement learn- ing for interference-aware path planning of cellular-connected uavs, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–7.
[32] F. Al-Turjman, J.P. Lemayian, S. Alturjman, L. Mostarda, Enhanced deployment strategy for the 5G drone-bs using artificial intelligence, IEEe Access. 7 (2019), 75 999–76 008.
[33] Y. Zeng, X. Xu, Path design for cellular-connected uav with rein- forcement learning, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–6.
[34] H. Bayerlein, P. De Kerret, D. Gesbert, Trajectory optimization for autonomous flying base station via reinforcement learning. 2018 IEEE 19th International Workshop On Signal Processing Advances in Wireless Communications (SPAWC), IEEE, 2018, pp. 1–5.
[35] U. Challita, W. Saad, and C. Bettstetter, "Cellular-connected uavs over 5 g: deep reinforcement learning for interference management," arXiv preprint *arXiv: 1801.05500*, 2018.
[36] M.A. Abd-Elmagid, A. Ferdowsi, H.S. Dhillon, W. Saad, Deep reinforcement learning for minimizing age-of-information in uav- assisted networks, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–6.
[37] A. Rodriguez-Ramos, C. Sampedro, H. Bavle, P. De La Puente, P. Campoy, A deep reinforcement learning strategy for uav autonomous landing on a moving platform, J. Intell. Robot. Syst. 93 (1–2) (2019) 351–366.
[38] Y. Ampatzidis, V. Partel, Uav-based high throughput phenotyping in citrus utilizing multispectral imaging and artificial intelligence, Remote Sens. (Basel) 11 (4) (2019) 410.
[39] Q. Cheng, X. Wang, J. Yang, L. Shen, Automated enemy avoid- ance of unmanned aerial vehicles based on reinforcement learning, Appl. Sci. 9 (4) (2019) 669.
[40] X. Liu, Y. Liu, Y. Chen, L. Hanzo, Trajectory design and power control for multi-uav assisted wireless networks: a machine learning approach, IEEe Trans. Veh. Technol. 68 (8) (2019) 7957–7969.
[41] S. Meng, X. Dai, B. Xiao, Y. Zhou, Y. Li, C. Gao, Deep learning–based fifth-generation millimeter-wave communication chan- nel tracking for unmanned aerial vehicle internet of things networks, Int. J. Distrib. Sens. Netw. 15 (8) (2019) 1550147719865882.
[42] N.K. Ure, G. Chowdhary, T. Toksoz, J.P. How, M.A. Vavrina, J. Vian, An automated battery management system to enable persistent missions with multiple aerial vehicles, IEEE/ASME Transact. Mech. 20 (1) (2014) 275–286.
[43] Y. Sun, D.W.K. Ng, D. Xu, L. Dai, R. Schober, Resource allocation for solar powered uav communication systems, in: 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), IEEE, 2018, pp. 1–5.
[44] P. Rajendran, H. Smith, Experimental study of solar module & maximum power point tracking system under controlled temperature conditions, Int. J. Adv. Sci. Eng. Inf. Technol. 8 (4) (2018) 1147–1153.
[45] H. Wang, J. Shen, Analysis of the characteristics of solar cell array based on matlab/simulink in solar unmanned aerial vehicle, IEEe Access. 6 (2018), 21 195–21 201.
[46] S. Morton, R. D'Sa, N. Papanikolopoulos, Solar powered uav: design and experiments, in: 2015 IEEE/RSJ international conference on intelligent robots and systems (IROS), IEEE, 2015, pp. 2460–2466.
[47] C. Wang, Z. Ma, Design of wireless power transfer device for uav, in: 2016 IEEE International Conference on Mechatronics and Automation, IEEE, 2016, pp. 2449–2454.
[48] M. Simic, C. Bil, V. Vojisavljevic, Investigation in wireless power transmission for uav charging, Procedia Comput. Sci. 60 (2015) 1846–1855.
[49] A.B. Junaid, Y. Lee, Y. Kim, Design and implementation of autonomous wireless charging station for rotary-wing uavs, Aerosp. Sci. Technol. 54 (2016) 253–266.
[50] T.M. Mostafa, A. Muharam, R. Hattori, Wireless battery charging system for drones via capacitive power transfer, in: 2017 IEEE PELS Workshop on Emerging Technologies: Wireless Power Transfer (WoW), IEEE, 2017, pp. 1–6.
[51] B. Saha, E. Koshimoto, C.C. Quach, E.F. Hogge, T.H. Strom, B.L. Hill, S. L. Vazquez, K. Goebel, Battery health management system for electric uavs, in: 2011 aerospace conference, IEEE, 2011, pp. 1–9.
[52] S. Park, L. Zhang, S. Chakraborty, Battery assignment and scheduling for drone delivery businesses, in: 2017 IEEE/ACM Inter- national Symposium on Low Power Electronics and Design (ISLPED), IEEE, 2017, pp. 1–6.
[53] K.A. Swieringa, C.B. Hanson, J.R. Richardson, J.D. White, Z. Hasan, E. Qian, A. Girard, Autonomous battery swapping system for small-scale helicopters, in: 2010 IEEE International Conference on Robotics and Automation, IEEE, 2010, pp. 3335–3340.
[54] B. Michini, T. Toksoz, J. Redding, M. Michini, J. How, M. Vavrina, J. Vian, Automated battery swap and recharge to enable persistent uav missions. Infotech@ Aerospace 2011, 2011, p. 1405.
[55] S. Dunbar, F. Wenzl, C. Hack, R. Hafeza, H. Esfeer, F. Defay, S. Prothin, D. Bajon, Z. Popovic, Wireless far-field charging of a micro-uav, in: 2015 IEEE Wireless Power Transfer Conference (WPTC), IEEE, 2015, pp. 1–4.
[56] X. Cao, P. Yang, M. Alzenad, X. Xi, D. Wu, H. Yanikomeroglu, Airborne communication networks: a survey, IEEE J. Selected Areas Commun. 36 (9) (2018) 1907–1926.
[57] V.S. Dwivedi, J. Patrikar, A. Addamane, A. Ghosh, Maraal: a low altitude long endurance solar powered uav for surveillance and mapping applications, in: 2018 23rd International Conference on Methods & Models in Automation & Robotics (MMAR), IEEE, 2018, pp. 449–454.
[58] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in uav communication networks, IEEE Commun. Surv. Tutorials 18 (2) (2015) 1123–1152.
[59] J. Chen, D. Gesbert, Optimal positioning of flying relays for wireless networks: a los map approach, in: 2017 IEEE international conference on communications (ICC), IEEE, 2017, pp. 1–6.

[60] F. Xu, T. Hong, J. Zhao, T. Yang, Detection and identification technology of rotor unmanned aerial vehicles in 5G scene, Internat. J. Distrib. Sensor Networks 15 (6) (2019) 1550147719853990.
[61] X. Ge, J. Wang, J. Ding, X. Cao, Z. Zhang, J. Liu, X. Li, Combining uav-based hyperspectral imagery and machine learning algorithms for soil moisture content monitoring, PeerJ. 7 (2019) e6926.
[62] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile internet and its applications in 5G era: a comprehensive review, Int. J. Commun. Syst. 32 (14) (2019) e3981.
[63] S. Tanwar, S. Tyagi, I. Budhiraja, N. Kumar, Tactile internet for autonomous vehicles: latency and reliability analysis, IEEe Wirel. Commun. 26 (4) (2019) 66–72.
[64] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, J.J. Rodrigues, Bheem: a blockchain-based framework for securing electronic health records, in: 2018 IEEE Globecom Workshops (GC Wkshps), IEEE, 2018, pp. 1–6.
[65] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, cryp- tography mailing list," 2009.
[66] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Informat. Sec. Applicat. 50 (2020) 102407.
[67] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, Blohost: blockchain enabled smart tourism and hospitality management, in: 2019 international conference on computer, informa- tion and telecommunication systems (CITS), IEEE, 2019, pp. 1–5.
[68] S.K. Singh, S. Rathore, J.H. Park, Blockiotintelligence: a blockchain-enabled intelligent iot architecture with artificial intelli- gence, Future Generat. Comp. Syst. 110 (2020) 721–743.
[69] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, J.J. Rodrigues, Tactile internet for smart communities in 5G: an insight for noma- based solutions, IEEe Trans. Industr. Inform. 15 (5) (2019) 3104–3112.
[70] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, J.J. Rodrigues, Diya: tactile internet driven delay assessment noma-based scheme for d2d communication, IEEe Trans. Industr. Inform. 15 (12) (2019) 6354–6366.
[71] D. Fang, Y. Qian, R.Q. Hu, Security for 5G mobile wireless networks, IEEe Access. 6 (2017) 4850–4874.
[72] A. Takacs, X. Lin, S. Hayes, E. Tejedor, Drones and networks: ensuring safe and secure operations, Ericsson White Paper 14 (2018).
[73] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, Overview of 5G security challenges and solutions, IEEE Commun. Stand. Magaz. 2 (1) (2018) 36–43.
[74] X. Wang, H. Liu, J. Zhang, J. Ren, S. Wang, S. Xu, Flowmap: a fine-grained flow measurement approach for data-center networks, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–7.
[75] M. Banerjee, J. Lee, K.K.R. Choo, A blockchain future for internet of things security: a position paper, Digit. Commun. Netw. 4 (3) (2018) 149–160.
[76] C.L. Krishna, R.R. Murphy, A review on cybersecurity vulner- abilities for unmanned aerial vehicles, in: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), IEEE, 2017, pp. 194–199.
[77] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, H. Janicke, Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes, J. Network Comp. Appl. 101 (2018) 55–82.
[78] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Au- thentication protocols for internet of things: a comprehensive survey," Security and Communication Networks, vol. 2017, 2017.
[79] E.F. Jesus, V.R. Chicarino, C.V. De Albuquerque, and A.A.d.A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," Security and Communication Networks, vol. 2018, 2018.
[80] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, et al., Overview of 5G security technology, Sci. China Informat. Sci. 61 (8) (2018) 1–25.
[81] I.J. Jensen, D.F. Selvaraj, P. Ranganathan, Blockchain technology for networked swarms of unmanned aerial vehicles (uavs), in: 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, 2019, pp. 1–7.
[82] M.A. Khan, K. Salah, Iot security: review, blockchain solutions, and open challenges, Fut. Generat. Comp. Syst. 82 (2018) 395–411.
[83] T. Lagkas, V. Argyriou, S. Bibi, P. Sarigiannidis, Uav iot frame- work views and challenges: towards protecting drones as "things, Sensors 18 (11) (2018) 4015.
[84] A. Mohsin, A. Zaidan, B. Zaidan, O.S. Albahri, A.S. Albahri, M. Al- salem, K. Mohammed, Blockchain authentication of network applications: taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions, Comp. Stand. Interfaces 64 (2019) 41–60.
[85] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: the challenges, and a way forward, J. Network Comp. Appl. 125 (2019) 251–279.
[86] M. Mozaffari, W. Saad, M. Bennis, Y.H. Nam, M. Debbah, A tutorial on uavs for wireless networks: applications, challenges, and open problems, IEEE Commun. Surv. Tutorials 21 (3) (2019) 2334–2360.
[87] Jin Xin, J. X., Li QianWen, L. Q., Zhao KaiXuan, Z. K., Zhao Bo, Z. B., He ZhiTao, H. Z., & Qiu ZhaoMei, Q. Z. (2019). Development and test of an electric precision seeder for small-size vegetable seeds.
[88] C. Corbari, R. Salerno, A. Ceppi, V. Telesca, M. Mancini, Smart irrigation forecast using satellite LANDSAT data and meteo-hydrological modeling, Agric. Water. Manage 212 (2019) 283–294.
[89] A.S.A. Ghafar, S.S.H. Hajjaj, K.R. Gsangaya, M.T.H. Sultan, M.F. Mail, L.S. Hua, Design and development of a robot for spraying fertilizers and pesticides for agriculture, Proceedings 81 (2023) 242–248.
[90] B. Allred, N. Eash, R. Freeland, L. Martinez, D. Wishart, Effective and efficient agricultural drainage pipe mapping with UAS thermal infrared imagery: a case study, Agric. Water. Manage 197 (2018) 132–137.
[91] M.P. Christiansen, M.S. Laursen, R.N. Jørgensen, S. Skovsen, R. Gislum, Designing and testing a UAV mapping system for agricultural field surveying, Sensors 17 (12) (2017) 270.
[92] D. He, N. Kumar, S. Zeadally, A. Vinel, L.T. Yang, Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries, IEEe Trans. Smart. Grid. 8 (5) (2017) 2411–2419.
[93] V. Ortega, F. Bouchmal, J.F. Monserrat, Trusted 5g vehicular net- works: blockchains and content-centric networking, IEEE Vehicular Techn. Mag. 13 (2) (2018) 121–127.
[94] N. Bozic, G. Pujolle, S. Secci, A tutorial on blockchain and applications to secure network control-planes, in: 2016 3rd Smart Cloud Networks & Systems (SCNS), IEEE, 2016, pp. 1–8.
[95] M.A. Rahman, M.S. Hossain, G. Loukas, E. Hassanain, S.S. Rahman, M. F. Alhamid, M. Guizani, Blockchain-based mobile edge computing framework for secure therapy applications, IEEe Access. 6 (2018), 72 469–72 478.
[96] Z. Yuan, J. Jin, L. Sun, K.W. Chin, G.M. Muntean, Ultra- reliable iot communications with uavs: a swarm use case, IEEE Commun. Magaz. 56 (12) (2018) 90–96.
[97] A. Kapitonov, S. Lonshakov, A. Krupenkin, I. Berman, Blockchain-based protocol of autonomous business activity for multi- agent systems consisting of uavs, in: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), IEEE, 2017, pp. 84–89.
[98] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustišek, Towards decentralized iot security enhancement: a blockchain approach, Comp. Electr. Eng. 72 (2018) 266–273.
[99] D. Kumar, P. Kumar, A. Ashok, et al., Introduction to multimedia big data computing for iot. Multimedia Big Data Computing for IoT Applications, Springer, 2020, pp. 3–36.
[100] P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned uav networks: challenges, solutions, and comparisons, Comp. Comm. 151 (2020) 518–538.
[101] V. Sharma, I. You, G. Kul, Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain, in: Proceedings of the 2017 international workshop on managing insider security threats, 2017, pp. 81–84.
[102] Z. Ma, W. Huang, W. Bi, H. Gao, Z. Wang, A master-slave blockchain paradigm and application in digital rights management, China Commun. 15 (8) (2018) 174–188.
[103] V. Sharma, I. You, F. Palmieri, D.N.K. Jayakody, J. Li, Secure and energy-efficient handover in fog networks using blockchain-based dmm, IEEE Commun. Magaz. 56 (5) (2018) 22–31.
[104] A. Dorri, S.S. Kanhere, R. Jurdak, Towards an optimized blockchain for iot, in: 2017 IEEE/ACM Second International Confer- ence on Internet-of-Things Design and Implementation (IoTDI), IEEE, 2017, pp. 173–178.
[105] C. Grasso, G. Schembra, Design of a uav-based videosurveillance system with tactile internet constraints in a 5G ecosystem, in: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), IEEE, 2018, pp. 449–455.
[106] X. Wang, A. Chowdhery, M. Chiang, Skyeyes: adaptive video streaming from uavs, in: Proceedings of the 3rd Workshop on Hot Topics in Wireless, 2016, pp. 2–6.
[107] D. He, N. Kumar, M.K. Khan, L. Wang, J. Shen, Efficient privacy-aware authentication scheme for mobile cloud computing ser- vices, IEEe Syst. J. 12 (2) (2016) 1621–1631.
[108] R. Amin, S.H. Islam, G. Biswas, M.K. Khan, N. Kumar, An efficient and practical smart card based anonymity preserving user authentication scheme for tmis using elliptic curve cryptography, J. Med. Syst. 39 (11) (2015) 1–18.
[109] J.R. Vacca, "Computer and information security handbook: morgan kauffman," Burlington, MA, p. 208, 2009.
[110] D. He, S. Chan, M. Guizani, Drone-assisted public safety net- works: the security aspect, IEEE Commun. Magaz. 55 (8) (2017) 218–223.
[111] S. Huh, S. Cho, S. Kim, Managing iot devices using blockchain platform, in: 2017 19th international conference on advanced commu- nication technology (ICACT), IEEE, 2017, pp. 464–467.
[112] S. Tanwar, S. Tyagi, N. Kumar, Security and privacy of electronic healthcare records: concepts, paradigms and solutions, Institution of Engineering and Technology, 2019.
[113] H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, Y. Lee, Blockonet: blockchain-based trusted cloud radio over optical fiber network for 5g fronthaul, in: Optical Fiber Communication Conference, Optical Society of America, 2018, pp. W2A–W25.
[114] H. Chao, A. Maheshwari, V. Sudarsanan, S. Tamaskar, D.A. DeLaurentis, Uav traffic information exchange network, in: 2018 Aviation Technology, Integration, and Operations Conference, 2018, p. 3347.
[115] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: the case study of a smart home, in: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, pp. 618–623.
[116] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M.S. Obaidat, A systematic review on security issues in vehicular ad hoc network, Sec. Privacy 1 (5) (2018) e39.
[117] D. Jones, Power line inspection-a uav concept, in: 2005 The IEE Forum on Autonomous Systems (Ref. No. 2005/11271), IET, 2005, 8–pp.
[118] G. Yang, J. Liu, C. Zhao, Z. Li, Y. Huang, H. Yu, B. Xu, X. Yang, D. Zhu, X. Zhang, et al., Unmanned aerial vehicle remote sensing for field-based crop phenotyping: current status and perspectives, Front. Plant Sci. 8 (2017) 1111.
[119] L.F. Luque-Vega, B. Castillo-Toledo, A. Loukianov, L.E. Gonzalez-Jimenez, Power line inspection via an unmanned aerial system based on the quadrotor helicopter,

in: MELECON 2014-2014 17th IEEE Mediterranean electrotechnical conference, IEEE, 2014, pp. 393–397.
[120] C. Sampedro, C. Martinez, A. Chauhan, P. Campoy, A supervised approach to electric tower detection and classification for power line inspection, in: 2014 International Joint Conference on Neural Networks (IJCNN), IEEE, 2014, pp. 1970–1977.
[121] Z. Li, Y. Liu, R. Walker, R. Hayward, J. Zhang, Towards automatic power line detection for a uav surveillance system using pulse coupled neural filter and an improved hough transform, Mach. Vis. Appl. 21 (5) (2010) 677–686.
[122] T. Dasu, Y. Kanza, D. Srivastava, Geofences in the sky: herding drones with blockchains and 5G, in: Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2018, pp. 73–76.
[123] R. Ferro, Y. Bernal, J. Tapicha, Technical development of a secu- rity platform for iot based on blockchain, in: International Conference on Knowledge Management in Organizations, Springer, 2018, pp. 625–633.
[124] K. Fan, Y. Ren, Y. Wang, H. Li, Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G, IET Commun. 12 (5) (2018) 527–532.
[125] A. Islam, S.Y. Shin, Buav: a blockchain based secure uav- assisted data acquisition scheme in internet of things, J. Commun. Networks 21 (5) (2019) 491–502.
[126] M. Clark, Robust wireless channel based secret key extraction, in: MILCOM 2012-2012 IEEE Military Communications Conference, IEEE, 2012, pp. 1–6.
[127] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, S. Martin, Blockchain based trust management mechanism for iot, in: 2019 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2019, pp. 1–8.
[128] A. Dorri, S.S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
[129] V. Sharma, I. You, D.N.K. Jayakody, D.G. Reina, K.K.R. Choo, Neural-blockchain-based ultrareliable caching for edge-enabled uav networks, IEEe Trans. Industr. Inform. 15 (10) (2019) 5723–5736.
[130] B. Mafakheri, T. Subramanya, L. Goratti, R. Riggio, Blockchain- based infrastructure sharing in 5G small cell networks, in: 2018 14th International Conference on Network and Service Management (CNSM), IEEE, 2018, pp. 313–317.
[131] L. Xiao, Y. Xu, D. Yang, Y. Zeng, Secrecy energy efficiency maximization for uav-enabled mobile relaying, IEEe Trans. Green. Commun. Netw. 4 (1) (2019) 180–193.
[132] M. Pustišek, A. Kos, Approaches to front-end iot application de- velopment for the ethereum blockchain, Procedia Comput. Sci. 129 (2018) 410–419.
[133] C. She, C. Liu, T.Q. Quek, C. Yang, Y. Li, Ultra-reliable and low- latency communications in unmanned aerial vehicle communication systems, IEEE Transact. Comm. 67 (5) (2019) 3768–3781.
[134] M. Madden, T. Jordan, D. Cotten, N. O'Hare, A. Pasqua, S. Bernardes, The future of unmanned aerial systems (uas) for monitoring natural and cultural resources, Proceed. Photogramm. Week 15 (2015) 369–384.
[135] I. Smith, M. Lee, M. Fortneberry, R. Judy, Hisentinel80: flight of a high altitude airship, in: 11th AIAA Aviation Technology, Integra- tion, and Operations (ATIO) Conference, including the AIAA Balloon Systems Conference and 19th AIAA Lighter-Than, 2011, p. 6973.
[136] H. Kaushal, G. Kaddoum, Optical communication in space: challenges and mitigation techniques, IEEE Commun. Surv. Tutor. 19 (1) (2016) 57–96.
[137] G. Saggiani, F. Persiani, A. Ceruti, P. Tortora, E. Troiani, F. Giuletti, S. Amici, M. Buongiorno, G. Distefano, G. Bentini, et al., A uav system for observing volcanoes and natural hazards, in: AGU Fall Meeting Abstracts 2007, 2007. GC11B–05.
[138] A. McGonigle, A. Aiuppa, G. Giudice, G. Tamburello, A. Hodson, S. Gurrieri, Unmanned aerial vehicle measurements of volcanic carbon dioxide fluxes, Geophys. Res. Lett. 35 (6) (2008).
[139] T.F. Villa, F. Gonzalez, B. Miljievic, Z.D. Ristovski, L. Morawska, An overview of small unmanned aerial vehicles for air quality measurements: present applications and future prospectives, Sensors 16 (7) (2016) 1072.
[140] J. Curry, J. Maslanik, G. Holland, and J. Pinto, "Applications of aerosondes in the arctic, b. am. meteorol. soc., 85, 1855–1861," 2004.
[141] K. Whitehead, B. Moorman, C. Hugenholtz, Low-cost, on- demand aerial photogrammetry for glaciological measurement, Cryosphere Discuss. 7 (3) (2013).
[142] N. Gruschka, M. Jensen, Attack surfaces: a taxonomy for attacks on cloud services, in: 2010 IEEE 3rd international conference on cloud computing, IEEE, 2010, pp. 276–279.
[143] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, et al., Understanding the mirai botnet, in: 26th USENIX security symposium (USENIX Security 17), 2017, pp. 1093–1110.
[144] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, Ddos in the iot: mirai and other botnets, Computer. (Long. Beach. Calif) 50 (7) (2017) 80–84.
[145] T. Tyagi, Botnet of things: Menace to Internet of Things, LAP LAMBERT Academic Publishing, 2018.
[146] G. Kambourakis, C. Kolias, A. Stavrou, The mirai botnet and the iot zombie armies, in: MILCOM 2017-2017 IEEE Military Communi- cations Conference (MILCOM), IEEE, 2017, pp. 267–272.
[147] M.M. Aung, Y.S. Chang, Traceability in a food supply chain: safety and quality perspectives, Food Control 39 (2014) 172–184.
[148] A. Boghossian, S. Linsky, A. Brown, P. Mutschler, B. Ulicny, L. Bar- rett, et al., "Threats to precision agriculture," US Department of Homeland Security, Washington, DC, USA, Tech. Rep. 20181003a, 2018.
[149] M. Window, "Security in precision agriculture: vulnerabilities and risks of agricultural systems," 2019.
[150] J. West, A prediction model framework for cyber-attacks to precision agriculture technologies, J. Agricult. Food Informat. 19 (4) (2018) 307–330.
[151] S. Underwood, Blockchain beyond bitcoin, Commun ACM 59 (11) (2016) 15–17.
[152] A Kamilaris, A. Fonts, F.X. Prenafeta-Boldύ, The rise of blockchain technology in agriculture and food supply chains, Trends Food Sci. Techn. 91 (2019) 640–652.
[153] J. Lin, Z. Shen, A. Zhang, Y. Chai, Blockchain and iot based food traceability for smart agriculture, in: Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018, pp. 1–6.
[154] S. Awan, S. Ahmed, N. Safwan, Z. Najam, M. Hashim, T. Safdar, Role of internet of things (iot) with blockchain technology for the development of smart farming, J. Mech. Cont. Math. Sci. 14 (5) (2019) 170–188.
[155] L.S. Shabadi, H.B. Biradar, Design and implementation of iot based smart security and monitoring for connected smart farming, Int. J. Comput. Appl. 975 (8887) (2008).
[156] D.D. Abuan, A.C. Abad, J.B. Lazaro Jr, E.P. Dadios, Security systems for remote farm, J. Automat. Control Eng. 2 (2) (2014).
[157] H. Chi, S. Welch, E. Vasserman, E. Kalaimannan, A framework of cybersecurity approaches in precision agriculture, in: proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance. Acad. Conf. Publ. Int. Reading, UK, 2017, pp. 90–95.
[158] M.M. Jahn, W. Oemichen, G. Treverton, et al., "Cyber risk and security implications in smart agriculture and food systems," Accessed: Nov, vol. 14, p. 2019, 2019.
[159] C.J. Chae and H.J. Cho, "Enhanced secure device authentication algorithm in p2p-based smart farm system," *Peer-to-peer networking and applications*, vol. 11, no. 6, pp. 1230–1239, 2018.
[160] L. Barreto, A. Amaral, Smart farming: cyber security challenges, in: 2018 International Conference on Intelligent Systems (IS), IEEE, 2018, pp. 870–876.
[161] A. Geil, G. Sagers, A.D. Spaulding, J.R. Wolf, Cyber security on the farm: an assessment of cyber security practices in the united states agricultural industry, Internat. Food Agribusiness Manage. Rev. 21 (1030–2018–1811) (2018) 317–334.
[162] S.E. Duncan, R. Reinhard, R.C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert, R. Murch, Cyber- biosecurity: a new perspective on protecting us food and agricultural system, Front. Bioeng. Biotechnol. 7 (2019) 63.
[163] H.M. Kim, M. Laskowski, Agriculture on the blockchain: sustainable solutions for food, farmers, and financing, Supply Chain Revol. (2018). Barrow Books.
[164] C. Kempenaar, C. Lokhorst, E. Bleumer, R. Veerkamp, T. Been, F. van Evert, M. Boogaardt, L. Ge, J. Wolfert, C. Verdouw, et al., "Big data analysis for smart farming: results of to2 project in theme food security," Wageningen University & Research, Tech. Rep., 2016.
[165] S. Wolfert, L. Ge, C. Verdouw, M.J. Bogaardt, Big data in smart farming–a review, Agric. Syst. 153 (2017) 69–80.
[166] S. Khorsandroo, A.S. Tosun, Time inference attacks on software defined networks: challenges and countermeasures, in: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), IEEE, 2018, pp. 342–349.