Chapter 1
Paradigms to secure Green dynamic IOT edged UAV for sustainable digital Transition

Kussum
Assistant Professor
Chandigarh University, Mohali, Punjab, India
kussum.e13593@cumail.in

Himanshi Phour
Assistant Professor
Chandigarh University, Mohali, Punjab, India
himanshi.e13362@cumail.in

1.1 Introduction

Unmanned Aerial Vehicles (UAVs) can indeed play a role in facilitating a sustainable digital transition in various sectors. Here are a few ways in which UAVs can contribute to sustainability and digital transformation:

Infrastructure Monitoring: UAVs equipped with cameras, sensors, and advanced imaging technologies can be used to monitor and inspect critical infrastructure such as power lines, pipelines, bridges, and buildings. By regularly assessing the condition of infrastructure, potential issues can be identified early, leading to proactive maintenance and reducing the risk of failures or accidents. This helps optimize resource allocation and minimize the environmental impact of infrastructure operations.

Renewable Energy Development: UAVs can assist in the planning and development of renewable energy projects. They can be used to survey and analyze potential sites for solar or wind farms, mapping the terrain, and assessing the feasibility of installations. Additionally, UAVs can monitor the performance of existing renewable energy installations, aiding in maintenance and optimization to ensure maximum efficiency and output.

Precision Agriculture: UAVs equipped with multispectral or thermal cameras can provide valuable data for precision agriculture. They can collect high-resolution imagery and data about crop health, soil moisture levels, and nutrient distribution. This information enables farmers to optimize their use of resources, reduce chemical inputs, and improve crop yields, resulting in more sustainable farming practices.

Environmental Monitoring: UAVs can be employed for environmental monitoring, including tracking deforestation, detecting wildfires, monitoring wildlife populations, and assessing air and water quality. By collecting real-time data from remote or hazardous areas, UAVs can help identify and address environmental issues promptly, enabling more effective conservation efforts.

Connectivity and Communication: In areas with limited or no internet connectivity, UAVs can serve as communication relays. They can be equipped with communication equipment to provide temporary network coverage for disaster-stricken regions, remote communities, or during large events. This helps bridge the digital divide, enabling sustainable development and access to essential services.

Delivery and Logistics: UAVs can contribute to sustainable logistics and delivery operations. By replacing traditional delivery methods, such as trucks or motorcycles, with drones for small package transportation, carbon emissions can be reduced, especially in urban areas. This promotes eco-friendly last-mile delivery and reduces traffic congestion.

It is important to consider the regulations and guidelines governing UAV operations, including airspace management, safety measures, and privacy concerns. Adhering to these regulations ensures the safe and responsible integration of UAVs into various sectors, promoting sustainability and the digital transition.

1.2 Green IoT Communications

Green IoT communication refers to the use of Internet of Things (IoT) technologies and practices that minimize the environmental impact and promote sustainability. It focuses on reducing energy consumption, optimizing resource utilization, and minimizing waste in IoT systems. Here are some key aspects of green IoT communication:

A. Energy Efficiency: Green IoT communication aims to reduce energy consumption by IoT devices and networks. This can be achieved through various means such as optimizing device power management, using low-power components and protocols, and employing energy harvesting techniques to power IoT devices.

B. Communication Protocols: Choosing energy-efficient communication protocols is crucial for green IoT communication. Low-power wireless protocols like Zigbee, Z-Wave, and Bluetooth Low Energy (BLE) are preferred over power-hungry protocols like Wi-Fi or cellular networks when feasible. These protocols minimize energy consumption and extend the battery life of IoT devices.

C. Resource Optimization: Green IoT communication involves optimizing the utilization of network resources. This includes efficient routing algorithms that minimize data transmission distances, reduce congestion, and utilize network resources effectively. By optimizing resource usage, unnecessary data transfers and network overhead can be minimized.

D. Data Management and Analytics: Efficient data management and analytics play a vital role in green IoT communication. By employing intelligent data processing techniques, unnecessary data transmissions and storage can be reduced. Edge computing and fog computing can be leveraged to process data locally, minimizing the need for transmitting large volumes of data to centralized cloud servers.

E. Lifecycle Management: Green IoT communication emphasizes the responsible management of IoT devices throughout their lifecycle. This includes proper disposal and recycling of devices, using eco-friendly materials in manufacturing, and encouraging device upgradability to extend their lifespan.

F. Environmental Monitoring: IoT devices can be employed for environmental monitoring and conservation efforts. For example, smart sensors can monitor air quality, water resources, and energy consumption, providing valuable data for sustainable decision-making and resource management.

G. Sustainable Infrastructure: Designing IoT infrastructure with sustainability in mind is a crucial aspect of green IoT communication. Using renewable energy sources to power IoT networks, reducing carbon emissions in data centers, and promoting efficient network architectures all contribute to a greener IoT ecosystem.

Overall, green IoT communication aims to strike a balance between leveraging the benefits of IoT technology while minimizing its environmental footprint. By adopting energy-efficient practices, optimizing resource utilization, and implementing sustainable strategies, we can create a more environmentally friendly and sustainable IoT ecosystem.

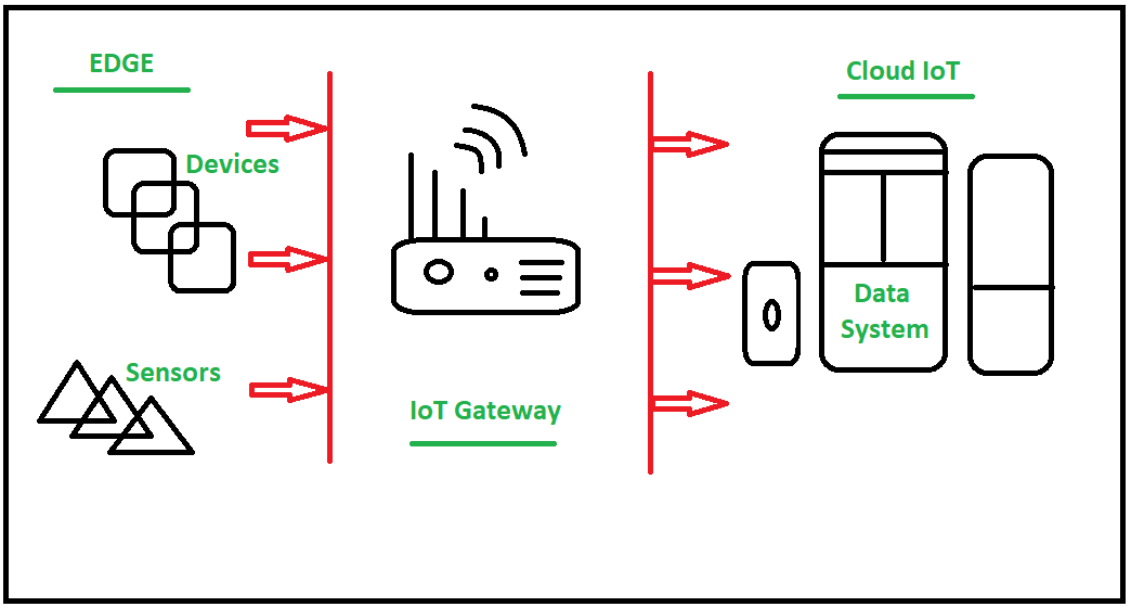

Figure 1.1: IoT gateway for the Internet connection

1.2.1 UAV-Empowered Edge Computing Environment

A UAV (Unmanned Aerial Vehicle) empowered edge computing environment refers to the integration of UAVs and edge computing technologies to enable efficient and distributed computing capabilities in remote or mobile environments.

In such an environment, UAVs are equipped with computing resources and act as mobile edge computing nodes. They can fly to remote locations or areas with limited infrastructure, bringing computational power and data processing capabilities closer to the data source. This concept leverages the advantages of both UAVs and edge computing to enable real-time data analysis, reduced latency, and improved scalability in various applications.

Here's an overview of how a UAV-empowered edge computing environment works:

A. UAVs as mobile edge computing nodes: UAVs are equipped with processing units, memory, storage, and communication capabilities. These resources enable UAVs to perform data processing tasks, such as running applications, analyzing sensor data, and executing algorithms.

B. Data collection and transmission: UAVs can be deployed to collect data from sensors, cameras, or other sources in their surroundings. The collected data can include images, videos, sensor readings, or any other relevant

information. The UAVs then process and analyze this data onboard, reducing the need for transmitting raw data to a centralized location.

C. Edge computing capabilities: UAVs act as edge computing nodes, which means they can perform computational tasks locally without relying on a centralized cloud infrastructure. They can execute algorithms, apply machine learning models, or perform real-time analytics directly onboard. This reduces latency and bandwidth requirements since only processed data or relevant insights are transmitted to the central system or other connected devices.

D. Communication and coordination: UAVs in the environment can communicate with each other and with a central control system. They can exchange information, synchronize their actions, and distribute computing tasks among themselves based on factors like proximity, computational load, or data relevance. This allows for efficient and distributed processing in the environment.

Applications of UAV-empowered edge computing environments include:

A. Disaster response and monitoring: UAVs can be deployed in disaster-stricken areas to collect real-time data, assess damage, and aid in search and rescue operations. The onboard edge computing capabilities enable rapid analysis of collected data, helping emergency responders make informed decisions on the ground.

B. Precision agriculture: UAVs equipped with sensors and edge computing capabilities can fly over agricultural fields, capturing data on crop health, soil conditions, or water usage. This data can be processed onboard to provide farmers with immediate insights, allowing them to optimize their operations and make timely interventions.

C. Surveillance and security: UAVs with edge computing capabilities can be used for surveillance and security purposes in public spaces, critical infrastructure, or large events. They can analyze video feeds, detect anomalies, or perform facial recognition locally, enhancing situational awareness and response time.

D. Industrial inspections: UAVs can inspect infrastructure such as pipelines, power lines, or wind turbines, capturing visual or sensor data. Onboard edge computing enables real-time analysis, identifying faults or anomalies, and reducing the need for extensive data transmission or human intervention.

UAV-empowered edge computing environments offer the advantages of mobility, real-time processing, reduced latency, and increased scalability. However, challenges such as limited battery life, payload capacity, and network connectivity in remote areas need to be addressed for effective implementation.

1.3 Open Security Pitfalls

In the emerging world of IoT based UAV fortune in the world of wireless which gives the new trends to find the pitfalls at the edge commuting devices . Mostly they lacks in security due to adhoc mobility and the security pitfalls which needs to be understand. Therefore to discuss their details below are the main security claims which efficiently sustain in the environment to compensate.

1.3.1 Security Challenges

Securing sustainability in IoT-edged UAV (Unmanned Aerial Vehicle) operations involves addressing various aspects related to environmental impact, energy efficiency, and responsible use of resources. Here are some considerations for achieving sustainability in IoT-edged UAV systems:

A. Energy Efficiency: Optimize the energy consumption of UAVs by using lightweight materials, efficient propulsion systems, and aerodynamic designs. Implement intelligent power management techniques, such as optimizing flight paths, payload utilization, and idle time, to minimize energy usage and increase flight endurance.

B. Renewable Energy Sources: Explore the integration of renewable energy sources, such as solar panels or fuel cells, to power UAVs. This approach can reduce dependence on conventional energy sources, lower emissions, and extend flight durations. Additionally, ground-based IoT infrastructure can be powered by renewable energy to support UAV operations.

C. Efficient Data Transmission: Enhance communication protocols and data transmission techniques between UAVs and IoT systems to minimize energy consumption. Utilize compression algorithms, data filtering, and edge computing capabilities to reduce the amount of data transmitted over the network, optimizing energy usage and improving bandwidth efficiency.

D. Responsible Manufacturing and Disposal: Promote sustainable manufacturing practices by using recyclable and environmentally friendly materials in UAV production. Implement proper disposal and recycling procedures to minimize the environmental impact of retired or damaged UAVs.

E. Environmental Monitoring: Leverage the capabilities of IoT sensors and edge computing on UAVs to monitor and collect environmental data. This data can be used for ecological studies, climate monitoring, and assessing the impact of human activities. By facilitating sustainable practices through data-driven insights, UAVs can contribute to environmental conservation efforts.

F. Regulatory Compliance: Ensure compliance with local regulations and guidelines for UAV operations to minimize disturbances to ecosystems and protected areas. Adhere to flight restrictions, noise limits, and privacy regulations to prevent negative impacts on wildlife, habitats, and communities.

G. Collaboration and Information Sharing: Foster collaboration among stakeholders, including UAV manufacturers, operators, regulators, researchers, and environmental organizations. Encourage the sharing of best practices, research findings, and technological advancements to promote sustainable development in the field of IoT-edged UAVs.

By addressing these considerations, the deployment of IoT-edged UAVs can be made more sustainable, minimizing their environmental footprint and promoting responsible use in various applications, such as environmental monitoring, disaster response, and infrastructure inspection.
IoT (Internet of Things) edged UAVs (Unmanned Aerial Vehicles) present unique security challenges due to their interconnected nature and reliance on both physical and digital systems. Here are some of the key security challenges associated with IoT edged UAVs:

A. Data Privacy: UAVs generate and collect vast amounts of data, including visual imagery, sensor readings, and location information. Ensuring the privacy of this data is crucial to prevent unauthorized access and misuse. Encryption and secure data transmission protocols should be implemented to protect sensitive information.

B. Unauthorized Access and Control: UAVs are vulnerable to unauthorized access by malicious individuals. If an attacker gains control of a UAV, they can manipulate its flight path, disrupt its operations, or even use it as a platform for launching cyber-attacks. Implementing strong authentication mechanisms, secure communication channels, and access controls can mitigate the risk of unauthorized access.

C. Network Vulnerabilities: IoT edged UAVs rely on wireless communication networks, making them susceptible to network-based attacks. Attackers may attempt to intercept or manipulate the UAV's communication channels, leading to data breaches, disruption of operations, or the injection of malicious commands. Securing the communication protocols, using encryption, and regularly updating firmware can help protect against such attacks.

D. Physical Security: UAVs are physically vulnerable to theft, tampering, or unauthorized modifications. Unauthorized access to the UAV's hardware can compromise its safety, integrity, and confidentiality. Physical security measures, such as secure storage, tamper-evident seals, and anti-tampering mechanisms, should be employed to protect against physical attacks.

E. Malware and Software Vulnerabilities: UAVs rely on complex software systems, including onboard flight controllers and ground control stations. These systems may contain vulnerabilities that could be exploited by attackers to compromise the UAV's operations or manipulate its behavior. Regular software updates, security testing, and code reviews are essential to identify and patch any vulnerabilities.

F. Interoperability and Standards: The IoT ecosystem comprises various devices and platforms from different manufacturers, each with its own set of protocols and standards. Ensuring interoperability and adherence to security standards across different components of an IoT edged UAV system can be a challenge. Lack of standardized security practices may create vulnerabilities and compatibility issues, increasing the risk of attacks.

G. Supply Chain Risks: The global supply chain for UAV components may involve multiple vendors and subcontractors, making it challenging to ensure the security and integrity of each component. Counterfeit or tampered parts could introduce vulnerabilities or compromise the overall security of the UAV. Implementing rigorous supply chain management processes, including trusted sourcing and verification, can help mitigate these risks.

To address these challenges, organizations developing IoT edged UAVs should adopt a holistic security approach. This includes implementing encryption, strong authentication mechanisms, secure communication protocols, regular software updates, physical security measures, and adhering to industry-recognized security standards. Continuous monitoring, vulnerability assessments, and threat intelligence should also be employed to identify and respond to emerging security threats effectively.

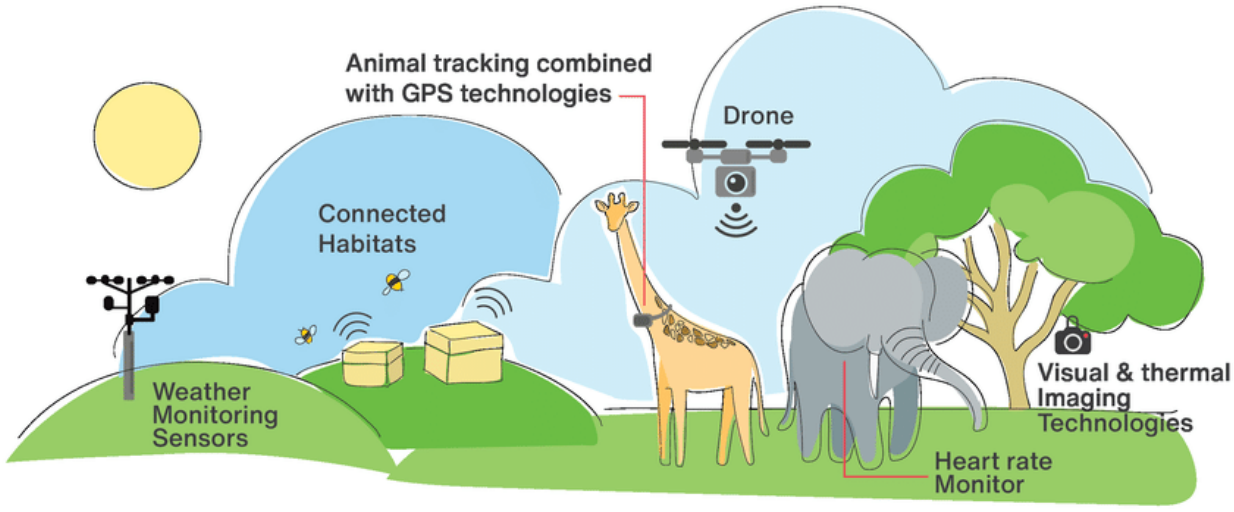

Figure 1.2: Use of IoT technology for research purposes on animal behavior

1.3.2 Data Driven Security in IoT

Data-driven security at the edges in AIOT (Artificial Intelligence of Things) based UAVs (Unmanned Aerial Vehicles) involves leveraging data analytics and machine learning techniques to enhance the security and privacy of these systems. The "edge" refers to the computing and processing capabilities located closer to the data source, which in this case would be the UAV.

Here are some key aspects of data-driven security at the edges in AIOT-based UAVs:

A. Anomaly detection: By collecting and analyzing data from various sensors and systems onboard the UAV, it becomes possible to identify anomalous behavior or deviations from normal patterns. This can help detect potential security threats such as unauthorized access, sensor tampering, or abnormal flight patterns.

B. Intrusion detection and prevention: Data-driven security systems can analyze network traffic and communication protocols to detect potential intrusions or malicious activities. By monitoring incoming and outgoing data packets, it becomes possible to identify and block unauthorized access attempts or suspicious network behavior.

C. Threat intelligence: By leveraging data from various sources, such as threat intelligence feeds or historical data, AIOT-based UAVs can enhance their security posture. This involves continuously updating and analyzing threat information to proactively identify and mitigate potential risks.

D. Secure communication: Ensuring secure communication channels between the UAV and ground control systems is crucial. Encryption techniques can be employed to protect data transmission, preventing unauthorized access or eavesdropping. Additionally, secure protocols and authentication mechanisms can be implemented to verify the integrity and authenticity of the communication.

E. Privacy preservation: UAVs often collect sensitive data, such as images or videos, during their operations. Data-driven security approaches can include techniques like differential privacy or data anonymization to protect the privacy of individuals or organizations involved. These methods aim to minimize the risk of re-identification of individuals or the disclosure of sensitive information.

F. Real-time decision-making: Leveraging machine learning algorithms, AIOT-based UAVs can analyze data in real-time to make informed security decisions autonomously. For example, the UAV can identify and respond to potential threats by adjusting its flight path, altering sensor configurations, or triggering alarms/alerts to the ground control system.

G. Data validation and integrity: Data-driven security mechanisms can include validation checks to ensure the integrity and authenticity of the collected data. This involves techniques like digital signatures or checksums to verify the data's origin and detect any tampering or corruption during transit or storage.

It's important to note that implementing data-driven security at the edges of AIOT-based UAVs requires careful consideration of computational resources, power constraints, and real-time processing capabilities. The architecture and design of such systems need to balance security requirements with the practical limitations of edge computing in UAVs.

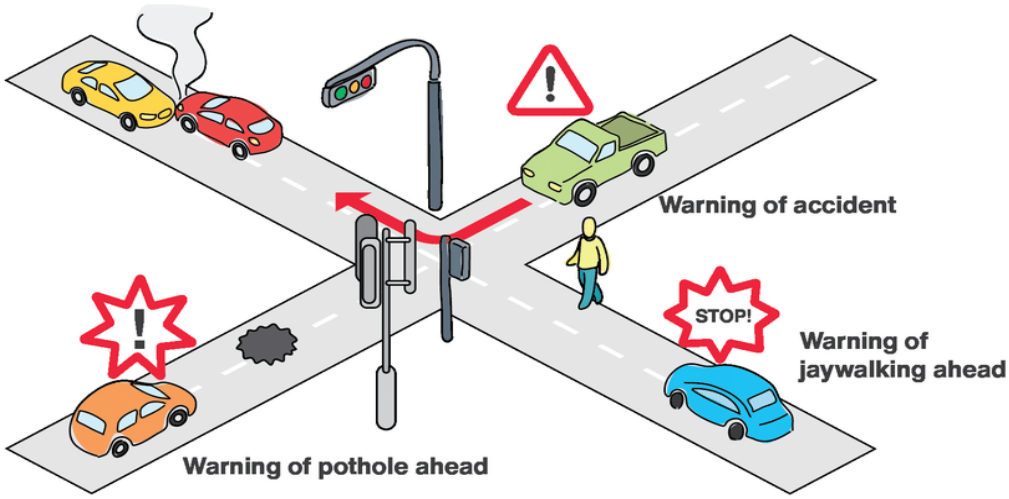

Figure 1.3: Connected street lighting pole as an IoT gateway to help drivers

1.3.3 Industrial Use Cases

AIOT (Artificial Intelligence of Things) refers to the integration of artificial intelligence (AI) technologies with the Internet of Things (IoT) devices. When it comes to UAV (Unmanned Aerial Vehicle) security, AIOT can be leveraged to enhance various industrial use cases. Here are some examples:

A. Surveillance and Intrusion Detection: AIOT-enabled UAVs equipped with cameras and sensors can autonomously monitor large industrial sites, critical infrastructure, or restricted areas. AI algorithms can analyze real-time video feeds and detect potential intrusions, unauthorized activities, or security breaches. The UAVs can send alerts or live video streams to security personnel for immediate action.

B. Perimeter Security: UAVs equipped with AIOT capabilities can patrol and monitor the perimeter of industrial facilities or sensitive areas. They can detect and respond to breaches, such as fence damage or unauthorized access attempts, by using AI algorithms to analyze sensor data and triggering alarms or notifications.

C. Asset Monitoring and Protection: AIOT-enabled UAVs can be deployed to monitor and protect valuable assets, such as equipment, machinery, or vehicles, in industrial settings. The UAVs can use AI algorithms to track asset locations, identify anomalies, and detect potential theft or damage. They can send real-time updates to security teams, allowing them to respond quickly to any security threats.

D. Emergency Response and Incident Management: In case of emergencies or incidents, AIOT-enabled UAVs can assist in the response and management process. For example, during a fire or hazardous situation, UAVs equipped with AI algorithms and sensors can provide real-time situational awareness, identify evacuation routes, or assess structural damage. This information can help emergency responders make informed decisions and allocate resources effectively.

E. Infrastructure Inspection: Industrial infrastructure, such as power lines, pipelines, or wind turbines, often requires regular inspections for maintenance and security purposes. AIOT-enabled UAVs can autonomously inspect these infrastructures, using AI algorithms to analyze sensor data and identify potential issues like damage, leaks, or structural weaknesses. This proactive approach helps ensure the integrity and security of critical industrial assets.

F. Airspace Monitoring: With the increasing use of UAVs, airspace security is becoming crucial. AIOT-enabled UAVs can contribute to airspace monitoring and control by employing AI algorithms to detect unauthorized or rogue drones. They can identify potential threats, track their movements, and assist in implementing countermeasures or conducting investigations if necessary.

G. Drone Dependent COVID-19 Medical Service: The researcher introduced a mechanism called DBCMS. During the covid-19 pandemic, the risk of being infected were high. Thus this medical service will reduce the risk of contamination for medical professionals. This solution has three layered architecture. In the first layer the drone will collect the samples. The second layer works on serious patients based upon samples collected and recommends the consultation of the doctors for emergencies and to control the pandemic situation the last layer warns the higher authorities. Therefore, in this hard situation drones were considered for surveillance purposes. The below figure shows how UAV can work during pandemic.

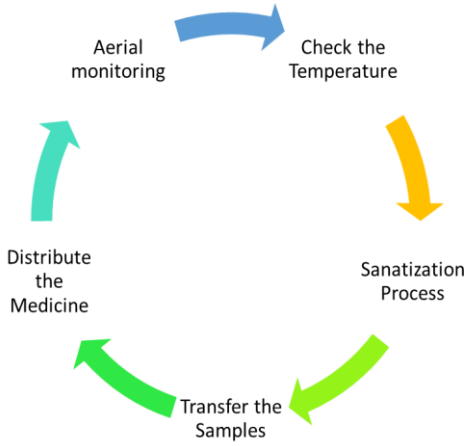

Figure 1.4: application of drone in covid

H. Thermal Cameras: Nowadays IOT based drones are equipped with thermal cameras to take the picture from the aerial spot. The service will also provide night time detection using night vision thermal cameras inbuilt drones. This technology allows the safe survey in the thermal areas in difficult scenarios. Number of case studies has been done by researchers which provide secure thermal images in which a drone will transfer the collected data on a mobile device server . Hence implementing the IOT in drones various applications can be performed without any human interference.

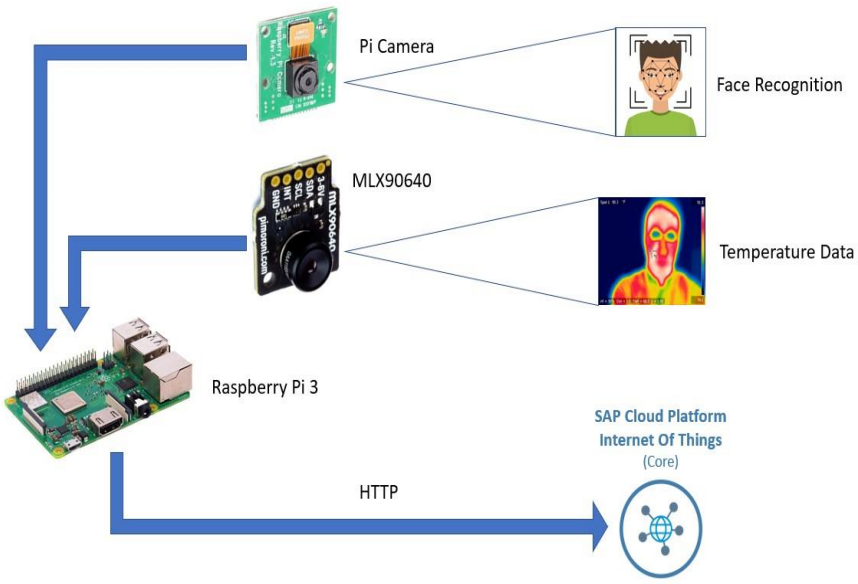

Figure 1.5: Application of ioT ebnaled thermal camera

I. UAV based IOV (Internet of vehicles): VANETs (Vehicular Ad Hoc Networks) is a type of vehicles that are based upon IOT technology, embedded with number of smart sensors and advanced software technologies. With the help of IOV transportation becomes more efficient, fast, safe as it comes with inbuilt smart sensors, by cutting the harmful gas emission it will be secure to the environment, moreover having the business benefits as well. Recently UAVs has shown great concern in IOV and VANETs. Implementing UAV with IOV brings numerous benefits to the mankind in the field of industry, military, transport, communication etc.

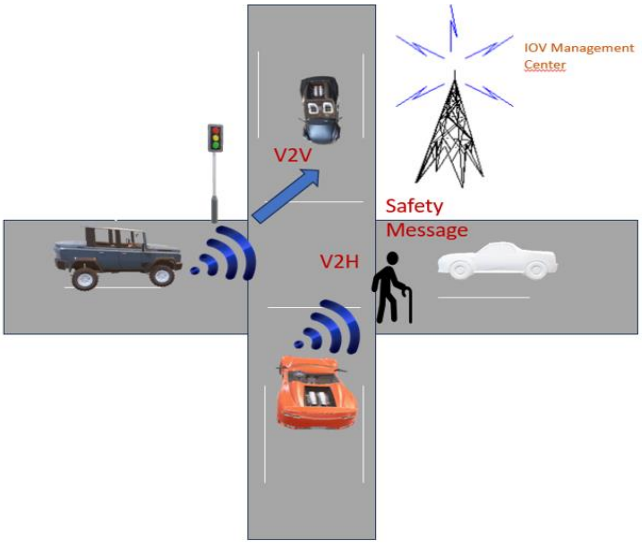

Figure 1.6: Application of IOT Enabled Vehicles

These are just a few examples of how AIOT-enabled UAVs can enhance security in industrial settings. The integration of AI technologies with UAVs and IoT devices opens up a wide range of possibilities for improving security, efficiency, and automation in various industries.

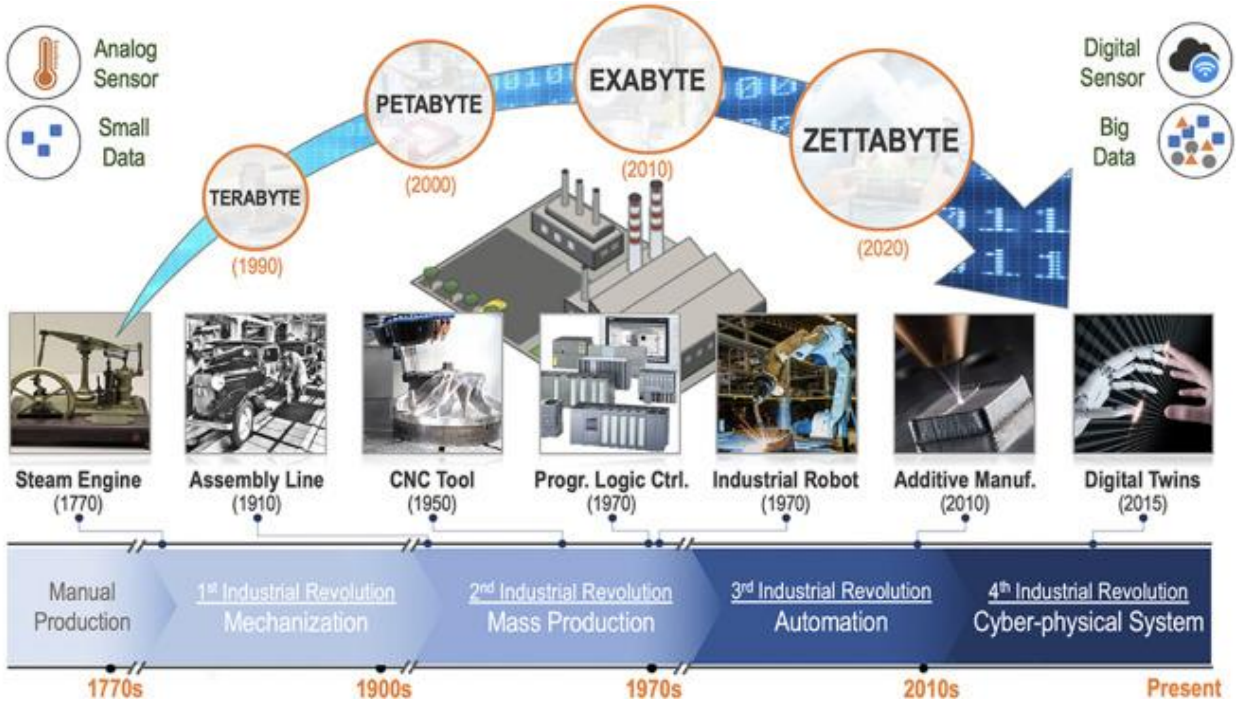

Figure 1.6: Welding robots in a smart factory generate huge amount of data

In public places such as stadiums or during parades, it is important to protect civilians from threats. Indeed, in recent years, the rate of crimes in urban areas, such as street crimes, vandalism, and terrorism, has increased. Therefore, anticipating crimes through detection and recognition of criminals among crowds of people is an important approach. In traditional patrol systems, there is a need for many security guards and a huge amount of human effort to provide necessary safety for people. In this vein, UAVs can be used to assist security guards by remotely surveilling people at places of interest. UAVs can provide immunity from any hazard and help not just to control but to track, detect, and recognize criminals adopting face recognition methods. Employing UAVs with appropriate IoT devices, such as video cameras, can offer an efficient crowd surveillance system; detect any eccentric motion and suspicious action; and recognize criminals' faces. The use of this technology provides a bird's eye view for crowd surveillance and face recognition. Therefore, crowd safety and security can be enhanced, while at the same time, the number of security guards deployed on the ground can be reduced. The process of face recognition consists of well defined steps: facial features extraction, database creation of known faces, and face detection matching videotaped faces with profiled ones. Different video analytic tools are available. Many of them can cope with the high mobility feature of UAVs and can achieve face recognition with high accuracy. Recognition of multiple faces at the same time is also possible. The processing of recorded video for face recognition can happen locally as well as at remote servers, enabling the offloading of the face recognition operation to MEC. OpenCV presents noticeable algorithms for face recognition. It employs machine learning to search for profiled faces within a video frame. Indeed, OpenCV uses LBPH with its associated libraries and databases. The approach of LBPH is to summarize the local structure in an image by comparing the pixels with its adjacent ones. LBPH results in accurate face recognition. In the remainder of this article, we demonstrate how much impact the offloading of face recognition computation has on the energy consumption of UAVs and the overall processing time. Figure 3 depicts the envisioned experiment scenario. In this

scenario, we consider a UAV equipped with a video camera and connected to the GCS through LTE cellular network. Figure 4a shows the UAV used in our experiment. The figure also shows the LTE eNodeB used (donated by Nokia). The underlying LTE network is exclusively used for research, and offers low latency and a high bit rate as well as extended coverage to support a variety of scenarios, where measurements can be carried out horizontally, vertically, at higher altitudes, with line of sight (LoS) and beyond LoS. The network includes edge computing resources co-located with the LTE base stations deployed in the Aalto University campus, thus enabling dedicated highspeed low-latency access to critical resources. This is schematically represented by MEC in Fig. 3. The used UAV is a built-in hexacopter equipped with an LTE modem, a gimbal with a high-resolution digital camera, as well as several computing and sensing resources. They include a flight controller (FC) module for stable flight, equipped with gyroscopes, accelerometers, and a barometer; and an embedded Linux system (i.e., a Raspberry Pi) interconnecting the LTE modem to the FC. To set up an LTE connection, any PC can be used as a GCS. On the PC, flight control software, such as Mission Planner, is installed. The PC is used for controlling the FC via a connected LTE modem. The hexacopter can carry 1.5 kg of payload, including laboratory equipment and metering devices. With a completely charged battery, its flight time is around 30 minutes with the full payload. It also has a safe landing scheme to cope with unlikely motor failure situations. In the envisioned scenario, security guards access the control station and continuously surveille the people. Upon noticing uncommon behavior from a particular person (or group of persons), they command the UAV to take a video of the person(s) and apply facial recognition on the captured video to identify the suspicious person(s) and verify if he/ she/they have any criminal records. To investigate the benefits of computation offloading of the facial recognition operation to MEC vs. its local processing, we developed a small-scale testbed as shown in Fig. 4b. The testbed environment consists of a Raspberry Pi (RPi) and a laptop that serves as a MEC node. The RPi works as the local processing unit onboard the UAV. In addition, the laptop works as the command and control station of the UAV's gateway for turning the camera on/off, or to command it to locally process the face recognition or offload the processing to the MEC node

1.3.4 IoT-edged Attracting Energy Efficient Security Mechanisms

When it comes to IoT devices, including edge devices, energy efficiency is crucial to ensure optimal performance and prolonged battery life. Security mechanisms are essential for protecting IoT devices and the data they handle. Here are some energy-efficient security mechanisms for IoT-edged devices:

A. Lightweight Cryptography: Traditional cryptographic algorithms can be resource-intensive for IoT devices. Lightweight cryptography refers to a set of cryptographic algorithms specifically designed to be computationally efficient, requiring less processing power and memory. By using lightweight cryptography algorithms, IoT-edged devices can perform encryption, authentication, and other security operations with reduced energy consumption.

B. Secure Bootstrapping: Secure bootstrapping ensures that IoT devices only communicate with trusted entities during the initial setup process. Instead of relying on complex and energy-consuming cryptographic protocols, lightweight and energy-efficient authentication methods can be employed. For example, using secure key exchange protocols like Elliptic Curve Diffie-Hellman (ECDH) can establish secure connections with minimal computational overhead.

C. Adaptive Security Levels: IoT-edged devices often operate in different environments with varying security requirements. By employing adaptive security levels, the devices can dynamically adjust their security mechanisms based on the context. For instance, in low-risk environments, the device may use minimal encryption or authentication, conserving energy. In high-risk scenarios, stronger security measures can be activated to ensure data protection.

D. Sleep/Wake Scheduling: IoT-edged devices can conserve energy by implementing sleep/wake scheduling mechanisms. These devices can periodically enter a low-power sleep mode when not actively engaged in

communication or processing tasks. Wake-up timers or event-based triggers can bring the device back to an operational state when needed, such as when security-related events occur or communication is required.

E. Data Aggregation and Filtering: IoT devices often generate a significant amount of data, which requires processing and transmission, consuming energy resources. Implementing data aggregation and filtering mechanisms at the edge can reduce the amount of data that needs to be processed and transmitted. By aggregating and filtering data at the device level, energy consumption can be minimized while ensuring that critical security-related information is retained.

F. Over-the-Air (OTA) Updates: Security vulnerabilities in IoT-edged devices can be addressed through OTA updates. Efficient OTA update mechanisms allow devices to receive security patches and firmware updates over the air. By employing delta updates, which only transmit the differences between the current and updated firmware versions, the energy consumption associated with downloading and installing updates can be significantly reduced.

G. Energy-Aware Protocols: IoT protocols, such as MQTT (Message Queuing Telemetry Transport) or CoAP (Constrained Application Protocol), can be adapted to incorporate energy-aware mechanisms. These mechanisms include strategies like minimizing packet size, reducing transmission frequency, and employing energy-efficient routing algorithms. By optimizing the communication protocols for energy efficiency, IoT-edged devices can reduce the overall energy consumption while maintaining secure communication.

Implementing these energy-efficient security mechanisms can help strike a balance between securing IoT-edged devices and conserving energy resources. By leveraging lightweight cryptography, adaptive security levels, sleep/wake scheduling, data aggregation, OTA updates, and energy-aware protocols, IoT-edged devices can maintain security while operating efficiently in resource.

1.3.5 IOT Edged Architecture

The Internet of Things (IoT) edge is a collection of applications and technologies which make it possible to interpret data and make choices in immediate time at an extent that would ordinarily be unachievable or very challenging to attain.The sheer quantity of data produced by Internet of Things (IoT) gadgets and the amount of computing resources needed to transfer and understand that data are just too much for current IT infrastructures to handle.Architectures for the Internet of Things(IoT) must develop as associated equipment and handheld gadgets increase in number.Combining edge computing with the Internet of Things (IoT) framework is the sole way to stay ahead of the curve.

As a way to cope with the data amount and movement, edge IoT(internet of things) layout transmits connectivity to networks from centrally located resources to the communications, resources, and conventional processing which are closer situated to the devices that are giving data to be processed.The categorization and simplification of transmission of information over the whole network are the primary objectives of moving to the edge. Data is analyzed as near to its initial stream as feasible in a distributed IT architecture known as edge computing.

IoT(internet of things) architecture includes processing data nearby, as opposed to transmitting it to the cloud or an on-site data center. The infrastructure and design concepts that enable data analysis, processing, and management at the borders of the the system, near (internet of things) IoT devices and detectors, as opposed to transmitting all data to a consolidated cloud for analyzing, are referred to as Internet of Things (IoT) Edge architecture.

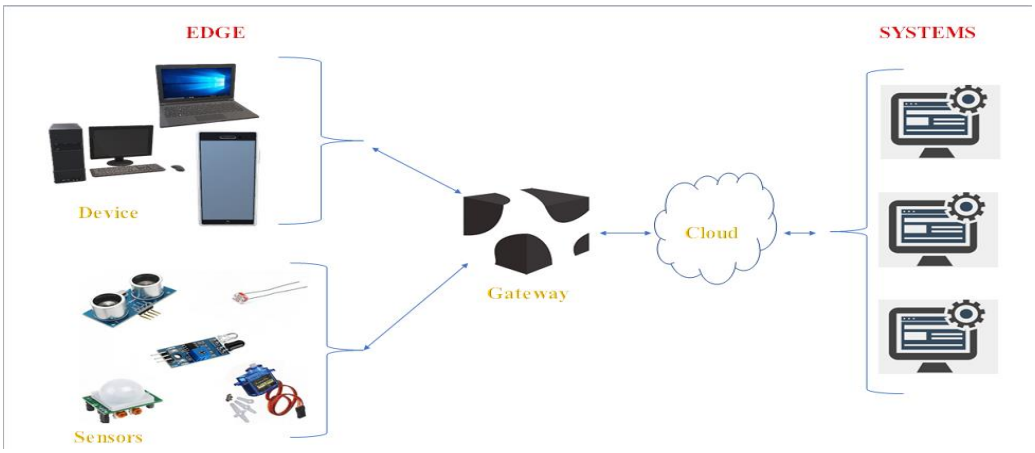

Figure 1.7: IOT Architecture

2. Algorithm to Secure iot Edge

Securing IoT (Internet of Things) edge devices is crucial to ensure the confidentiality, integrity, and availability of data and services.Security issues have grown as Internet of Things (IoT) technology has become more widely used. Since most IoT devices have limited computing power, encryption appears to be a workable solution for data protection. This article examines the various encryption algorithms and how they work.

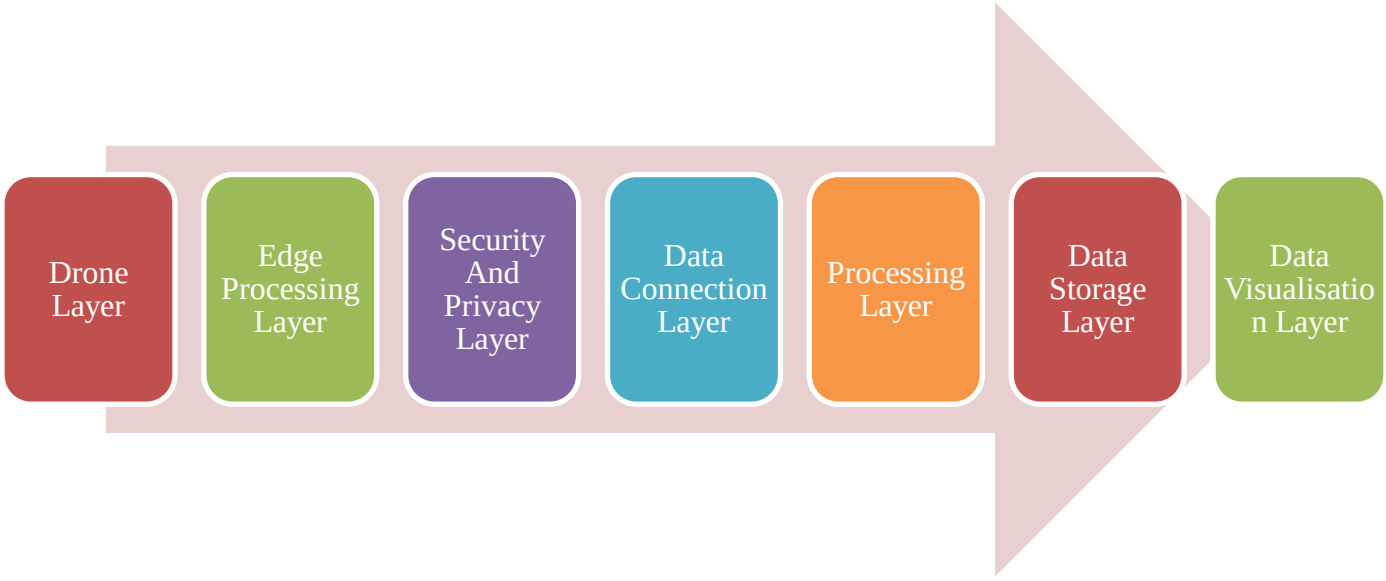

Figure 2.1: IOT Layered Architecture

In order to address drone security risks such data interception, data privacy, and typical cybersecurity threats, this research primarily focused on improving the fundamental design of drones. To facilitate the integration of security and data analysis mechanisms in the conventional drone's architecture, additional levels are incorporated in the suggested approach's layer design.

The layer architecture will be improved, enabling simple regeneration for upcoming improvements. Fig. 2 illustrates the installation of a security and privacy layer together with an update to the data processing layer using machine intelligence components.

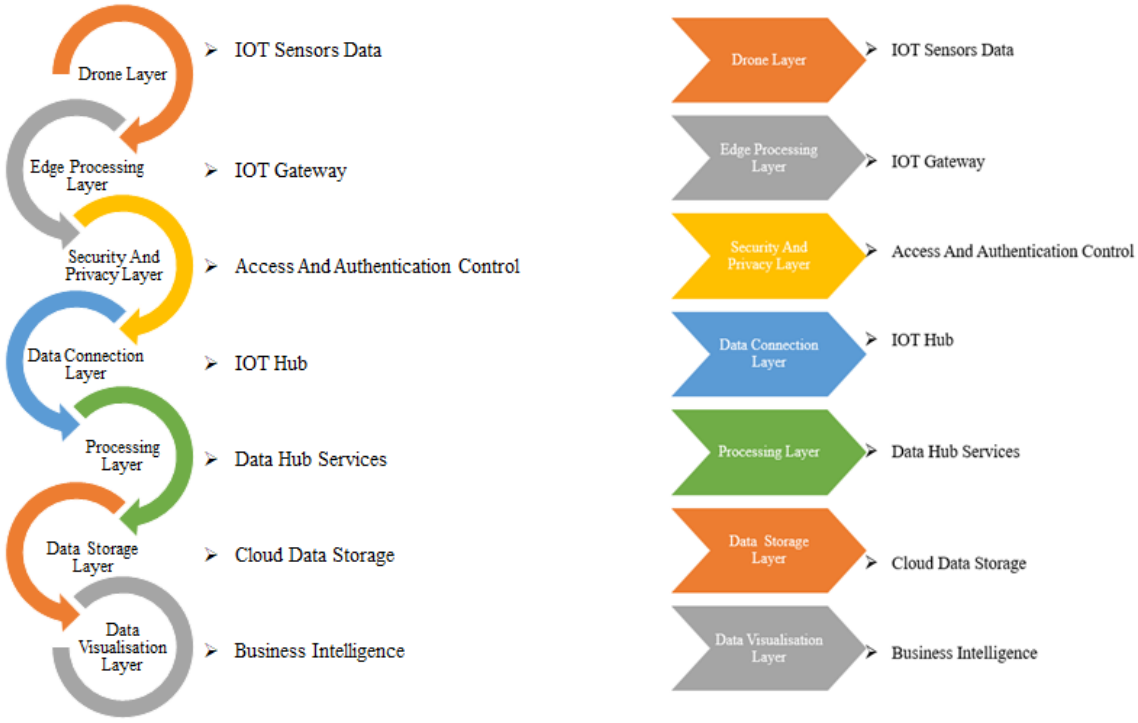

Figure 2.2: IOT Edge Architecture

A. Edge Processing Layer

This layer transmits drone and IoT raw data to the security and privacy layer, which verifies the data's source as coming from authorised devices. In this layer, wireless connection that enables quick information transfer is provided by IoT gateways. This layer is in charge of preserving, flooding, and cashing data. It utilises the Azure IoT gateway to communicate with the cloud.

B. Drone Layer

The tiny drone or quadcopter that has to be attached with a camera forms the initial layer of industrial drones. Smart sensors including an altitude sensor, radar, GPS sensor, and camera are employed in this layer. This layer's function is to perceive, record, and transfer drone-collected data to the following layer. A DJI phantom 3 drone with a modified remote controller and communication link has been launched.

C. Security and Privacy Layer

By using machine learning methods, this layer secures access control while providing authentication to the devices. Some privacy risks, including those involving physicality, behaviour, and location, are present in this layer.

The drone data that affects a compromised person's personal information is discreetly observed and collected by a third party. Unauthorised individuals are able to observe the actions and behaviour of others while behaviour privacy

is in place. Threats based on location privacy require authorised individuals obtaining the location. Through the use of authentication mechanisms, these dangers may be controlled. Device authentication also use machine learning techniques to notify and identify security threats.
The goal of edge computing is to bring applications and processing power as near as possible to the people or "objects" that require them. The growth in connected devices on the Internet of Things (IoT) and the lower cost of computer components are the main factors driving edge computing and mobile computing. Time-sensitive data in Edge Computing may be handled by a smart device or transmitted to a medium server nearby depending on the application. Edge computing is the end-to-end encryption-based optimisation of the data used by the application. In other words, cloud computing transforms the existing computing cloud architecture. In the near future, edge computing is anticipated to have a significant impact, particularly in terms of information technology.

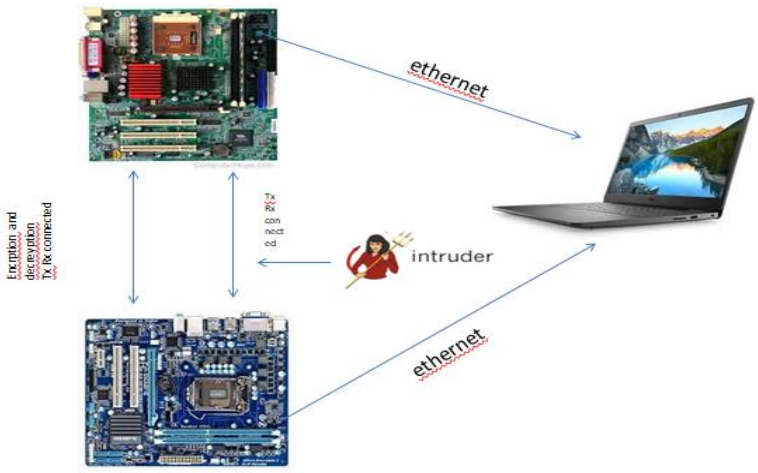

Figure 2.3: IOT Security

This study aims to encrypt data transmitted from IoT devices. In this investigation, Arduino devices. While the second one was utilised to obtain sensor data, the first one served as a gateway device.

To get information from the physical surroundings, a DHT11 sensor is employed.

Data from the sensor will be transmitted to the network gateway after being encrypted with AES 128. IoT devices will therefore be able to send secure data. Additionally, Arduinos may interact with one another. There is a wired connection.

Demonstrates the connections between all the elements required for the procedure. The laptop receives and encrypts the sensor data from Arduino 1. Additionally, a gateway is sent from Arduino 2 to Arduino 1 once again. After that, Arduino 1 is unlocked.
Encrypting the data serves as a safeguard against malicious software as it travels from one device to another.

A BCT-based method to lower the risks associated with data upkeep in UAV and drone systems is presented in the current work. To be more precise, this strategy aims to offer improved data storage and privacy methods that include special characteristics like immutability, tamper-proofing, transparency, security, and efficient distribution systems.

Drone, UAV, and IoT devices typically have a variety of sensors that assist in carrying out certain activities based on user preference.

3 Open challenges

Although this chapter deeply discussed the experimental applications of IOT based UAV as this will have the major impact on our society, however these applications also have some drawbacks that will require modification. Some of the major risks to the IOT based drones are given below:

A. Risk of Security: The susceptibility to cyber security threats is one of the main issues that IoT-based UAVs must deal with. Due to their internet connectivity, these gadgets can be vulnerable to hacking and illegal access. This may result in unauthorized access to private information, tampering with remote controls, or even UAV hijacking.

B. Regulatory Challenges: As the usage of IoT-based UAVs grows, regulatory issues relating to airspace management, privacy, and adherence to aviation regulations are raised. Some of the challenges to be faced include ensuring safe operation in congested airspace, addressing privacy issues over data collecting by UAVs, and modifying rules to keep up with technical advancements.

C. Issues with bandwidth and communication: Frequencies are critical because they affect the effectiveness of the IoT-based UAVs' interactions with ground control systems. But many places still don't have adequate network coverage, which makes it difficult to keep a steady connection going and provide real-time data. The amount of data that may be transmitted between the UAV and the ground control may also be constrained by bandwidth restrictions.

D. Battery Life and Energy Consumption: IoT-based UAVs need a constant source of electricity to assure their operations, hence they have limited battery life. The UAVs' and their IoT sensors' energy requirements, however, can be a serious obstacle. In order to allow longer flight lengths and greater functionality, it is crucial to find solutions to optimize energy usage and boost battery life.

E. Integration and Interoperability: In order for IoT-based UAVs to function properly, there must be seamless integration and interoperability between various systems and technologies. To efficiently transmit information, UAVs must be able to interface with a variety of sensors, equipment, and platforms. It might be difficult to ensure interoperability and established protocols among various IoT devices, especially when working with different manufacturers and technologies.

F. Malware: Any Internet of Things (IoT) device, including drones and unmanned aerial vehicles (UAVs), is at risk from malware. Protecting these devices against malware is crucial given the rise in the use of drones for a variety of tasks, including surveillance, delivery, and agriculture, in order to avoid security breaches or unauthorized access.Malware has the ability to intercept or change the data that is transmitted between a drone's control systems and the drone itself. Information leakage, data manipulation, and privacy violations may result from this. Also, Drones that have been infected with malware can be used as part of a botnet, which is an attack-controlled network of hacked devices. This can be used to start malicious actions like distributed denial-of-service (DDoS) attacks.

Therefore, it is crucial to ensure the security of IoT devices. A number of steps must be done to ensure the security of IoT devices. IoT devices must first be used with greater security performance, and they must be fully protected by security measures. Second, in order to prevent known security vulnerabilities, IoT devices need to have frequent

upgrades and maintenance performed on their systems and software. Additionally, encryption is necessary to safeguard IoT device connection in order to guard against data theft and tampering.

Conclusion and future scope

The focus of the current study is employing blockchain technology to solve concerns about data privacy and data preservation in IoT devices, UAVs, and drone applications. The effectiveness of the suggested application is assessed in comparison to the outcomes obtained following the adoption of BCT-based IoT applications vs conventional systems. The outcomes support the model's superiority.

Security Solutions including quantum cryptography, lightweight schemes, blockchain-based solutions, and trajectory planning, etc. The safe communication network between UAVs is examined in this paper by methodically responding to research questions based on the research technique used for the pertinent study. Finally, the paper discusses a number of points and offers suggestions for further study.

References

[1]. Jatin Sharma, Pawan Singh Mehra,Secure communication in IOT-based UAV networks: A systematic survey,Internet of Things,2023,100883,ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100883.

[2]. . Rupa Ch, Gautam Srivastava, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Sweta Bhattacharya,Security and privacy of UAV data using blockchain technology,Journal of Information Security and Applications,Volume 55,2020,102670, ISSN 2214-2126,https://doi.org/10.1016/j.jisa.2020.102670

[3]. Nayyar, A., Nguyen, B. L., and Nguyen, N. G., “The Internet of Drone Things (IoDT): Future Envision of Smart Drones”, International Conference on Sustainable Technologies for Computational Intelligence. Springer, Singapore. pp. 563-580, 2020.

[4]. R. Koslowski and M. Schulzke, "Drones along borders: border security UAVs in the United States and the European Union", International Studies Perspectives, vol. 19, pp. 305-324, 2018. 5. Trevor Hastie, R. T., Jerome Friedman. The Elements of Statistical Learning. 2009.

[5]. C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, “Security and privacy for the internet of drones: Challenges and solutions”, IEEE Communications Magazine, vol. 56, no.1, pp. 64-69, 2018.

[6]. R. Lombreglia, “The Internet of things,” Boston Globe, pp. 76–83, 2005.

[7]. M. F. Mushtaq, U. Akram, I. Khan, S. N. Khan, A. Shahzad and A. Ullah, “Cloud Computing Environment and Security Challenges: A Review” International Journal of Advanced Computer Science and Applications, vol. 8, no. 10, 2017.

[8]. Yoney Kirsal Ever.

[9]. A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications, Computer Communications,Volume 155,2020,Pages 143-149,ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2020.03.009. (https://www.sciencedirect.com/science/article/pii/S014036641930790X).

[10]. M. Singh and S. Sankaran, "Lightweight Security Architecture for IoT Edge Devices," *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*, Warangal, India, 2022, pp. 455-458, doi: 10.1109/iSES54909.2022.00099.

[11]. K. Liu, M. Yang, Z. Ling, H. Yan, Y. Zhang, X. Fu, et al., "On manually reverse engineering communication protocols of linux-based iot systems", *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6815-6827, 2020.

[12]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.

[13]. M. Sabt, M. Achemlal and A. Bouabdallah, "Trusted execution environment: what it is and what it is not", *2015 IEEE Trust-com/BigDataSE/ISPA*, vol. 1, pp. 57-64, 2015.

[14]. R. T. Tiburski, C. R. Moratelli, S. F. Johann, M. V. Neves, E. de Matos, L. A. Amaral, et al., "Lightweight security architecture based on embedded virtualization and trust mechanisms for iot edge devices", *IEEE Communications Magazine*, vol. 57, no. 2, pp. 67-73, 2019.

[15]. J. Wang, H. Li, J. Ye and J. Xiao, "Research on Intelligent Reverse Analysis Technology of Firmware of Internet of Things," *2021 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, Shenyang, China, 2021, pp. 164-169, doi: 1109/ICPICS52425.2021.9524146.

[16]. M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. K. A. Khalid, and M. M. Deris, “Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes,” J. Telecommun. Electron. Comput. Eng., vol. 9, no. 3–4, pp. 195–200, 2017.

[17]. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, “Evaluation of machine learning classifiers for mobile malware detection,” Soft Computing, vol. 20, no. 1, pp. 343–357, 2016. 17. D. Hussain, M. A. Khan, S. Abbas, R. A. Naqvi, M. F. Mushtaq, A. Rehman and A. Nadeem, “Enabling Smart Cities with Cognition Based Intelligent Route Decision in Vehicles Empowered with Deep Extreme Learning Machine”, Computers, Materials & Continua, 2020.

[18]. V. Chang, P. Chundury, and M. Chetty, “Spiders in the sky: User perceptions of drones, privacy, and security”, Proceedings of the 2017 CHI conference on human factors in computing systems, 2017.

[19]. D. Rahbari, S. Kabirzadeh and M. Nickray, "A security aware scheduling in fog computing by hyper heuristic algorithm," *2017 3rd Iranian Conference on Intelligent Systems and Signal Processing (ICSPIS)*, Shahrood, Iran, 2017, pp. 87-92, doi: 10.1109/ICSPIS.2017.8311595.
[20]. F. A. Kraemer, A. E. Braten, N. Tamkittikhun and D. Palma, "Fog computing in healthcare-a review and discussion", *IEEE Access 2017*.
[21]. C. Puliafito, E. Mingozzi and G. Anastasi, "Fog computing for the internet of mobile things: issues and challenges" in g: A review and a conceptual live vm migration framework", *Smart Computing (SMARTCOMP) 2017 IEEE International Conference*, pp. 1-6, 2017.
[22]. Z. Li, J. Ge, H. Yang, L. Huang, H. Hu and B. Luo, "A security and cost aware scheduling algorithm for heterogeneous tasks of scientific workflow in clouds", *Future Generation Computer Systems*, vol. 65, pp. 140-152, 2016.
[23]. T. Mathew, K. C. Sekaran and J. Jose, "Study and analysis of various task scheduling algorithms in the cloud computing environment", *Advances in Computing Communications and Informatics (ICACCI 2014 International Conference*, pp. 658-664, 2014.
[24]. Kumar, M., Mukherjee, P., Verma, S. *et al.* A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm. *Sci Rep* 13, 5372 (2023). https://doi.org/10.1038/s41598-023-32098-2.
[25]. Yongling Lu, Zhen Wang, Chengbo Hu, Ziquan Liu, Xueqiong Zhu, "Edge Computing Server Placement Strategy Based on SPEA2 in Power Internet of Things", *Security and Communication Networks*, vol. 2022, Article ID 3810670, 11 pages, 2022. https://doi.org/10.1155/2022/3810670.
[26] Atefeh Hemmati, Mani Zarei, Alireza Souri: UAV-based Internet of Vehicles: A Systematic Literature Review, April 2023.
[27] Yalin Liu, Hong -Ning Dai, Qubeijian Wang, Mahendra K. Shukla, Muhammad Imran, Unnamed Aerial Vehicle for Internet of Everything :Opportunities and Challenges, Science Direct.
[28] Internet of Vehicles(IOV), Eastern Peak.