1. INTRODUCTION

Unmanned aerial vehicles (UAVs), also referred to as drones, are aircraft that do not require a human pilot. The drone industry in India is still in its infancy stage, but it is expected to grow and evolve over the next few years. At present, drones are widely used in military and commercial applications such as surveillance, crop protection, construction project surveying, filmmaking, healthcare, e-commerce delivery, and more.

Since traditional methods are sometimes time-intensive and prone to human error, utilising drones in their place can result in considerable cost savings and mass adoption while enhancing the value of information obtained.

Thus, several start-ups and companies are currently involved in developing and identifying new applications and use cases for drones. And this is driving the drone industry further. Additionally, start-ups in India are focusing on improving and advancing their technological capabilities, while corporations are heavily investing in the drone ecosystem. However, cybersecurity issues associated with drone applications present themselves as a constraint, and thus, the government has imposed prohibitions or restrictions on drone possession and imports.

1.1. Purpose

When drone was first introduced in India, they were mainly used as defence equipment, but the applications have gradually expanded since then. Along with the growing applications, the market size has also been growing. It was estimated that by the year 2030, the Indian drone market in India would reach 2.5 trillion Indian rupees.

By the end of 2023, there were more than 13 thousand drones registered in India. During the same period, the Directorate General of Civil Aviation (DGCA) authorized 70 drone pilot training facilities in the country, with close to eight thousand pilots trained. Outside the military and security applications, more and more drones have been used in civilian capacities.

Drones have been repeatedly utilized to infringe on user privacy. The number of attacks targeting drones is also increasing and therefore more research is

needed. However, privacy has not been explored from the perspective of the drone owner. The drone owner, e.g., a hobbyist, is a user who is accountable and responsible for the drone. We are interested in studying what consequences the drone owners face when their privacy is compromised as well as what skills and capabilities are needed to execute a drone attack. Specifically, we want to achieve the mentioned objectives through a de-authentication attack and execute it against a commercial drone by utilizing open-source software. A de-authentication attack exploits the communication between a user and an access point. The attack sends disassociate frames to the access point, on behalf of the user, causing the connection to the user to terminate. De-authentication attacks can be potentially run without needing a person (the attacker) to be in proximity of the drone. Thus, this makes this attack class interesting to study against drones, particularly from a privacy perspective.

2. LITERATURE SURVEY

2.1. Vulnerabilities and Attacks Analysis for Military and Commercial IoT Drones

The integration of HD cameras and Wi-Fi features has caused a new type of vulnerability to cyber threats like jamming and video replay attacks in military and commercial drones. KilToys Camera Drone and Cheerwing Syma X55W-V3 FPV Eplores2 among other drones were experimented on during the study, using drones with Wi-Fi connectivity for testing detection, information gathering, and exploit capabilities.

It also covers the problem of regulation regarding UAVs, where Congress tasked FAA to formulate regulations concerning UAVs in the National Airspace System by 2025. A major difficulty that FAA faces in drone regulation is cybersecurity such as GPS spoofing and network intrusions. Risk assessment formula evaluates risks associated with drone vulnerabilities comparing probability associated with distinct types of attacks on commercial and military drones. The paper finally emphasizes mitigation strategies that should be put in place to address these vulnerabilities so that business can continue even after an attack occurs.

Additionally, it examines various vulnerabilities affecting drones, including jamming, GPS spoofing, packet sniffing, de-authentication, and video replay attacks. It discusses the use of tools to analyse drones' Wi-Fi capabilities and the execution of attacks like jamming and GPS spoofing. Proposed mitigation tactics aim to counteract drone attacks by advocating for multiple contingency plans to prevent single points of failure. The study also highlights the potential for attackers to seize control of drones by exploiting vulnerabilities, underscoring the significance of recognising and defending against such threats in military and commercial drone operations.

2.2. System to capture WiFi based Drones using IoT

It explores how the IoT technology is integrated into drones' control, pinpointing some of the benefits that come with it such as convenience and efficiency in various tasks. Being unmanned aerial vehicles, drones can be managed through WiFi transmissions or radio frequency signals hence they can be used to do any form of work whether legal or illegal. The paper highlights the necessity for anti-drone systems which can manage security challenges due to misuse of drones especially in smart city environments. Nonetheless, existing high-cost anti-drone technologies restrict their civilian application leading to an investigation of an IoT-based system using Raspberry Pi and Wifi-Pineapple for drone control.

It looks at wireless attacks specifically related to de-authentication attacks and password cracking on Wi-Fi-enabled drones. Experiments were performed on a DJI Tello drone evidencing that these types of attacks are effective at severing connection between the pilot and the drone. The success rate was noted at approximately 55% while insights into the drone's channel-changing activities impacted on results of this attack. In addition, there is a section detailing future work which will include integration of more wireless attacks, testing on drones from different manufacturers, and making the system more adaptable to drone responses.

Furthermore, the proposed anti-drone system involves a mechanism where the system continuously scans for WiFi signals in its vicinity and initiates an attack when a drone enters its range. The system employs brute force attacks to crack passwords, locate the drone's IP address, obtain the MAC address, and launch

de-authentication attacks to bring down the drone. By automating these processes, the system aims to enhance security measures against unauthorized drone activities and protect sensitive areas from potential drone threats.

2.3. Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures

It shows many facets of drones, including their great progress and the risks they have. For instance, the various kinds of drones are discussed here such as fixed-wing, rotary-wing and hybrid-wing drones, where each type is known to possess unique application and capability. Autonomous control, supervised control and pilot control represent the autonomy spectrum in which different levels of human interaction are visible during these gadgets' operations.

One of the key issues highlighted in this study is security flaws that exist within drone systems like flight controllers and ground control stations that can be utilized for physical or cyber-attacks. Furthermore, reliance on sensors by drones to operate accurately may also be subject to manipulation of sensor data by malicious actors for purposes of interfering with flight activities thereby stressing the need for safeguarding sensor information.

Furthermore, it discusses potential threats and attacks that drones may face, ranging from GPS spoofing attacks to data interception in wireless sensor networks. It also explores countermeasures to mitigate these risks, including the use of Blockchain, Machine Learning, Fog Computing, and Software Defined Networks as protective measures against security breaches. By addressing these security challenges and implementing robust countermeasures, stakeholders in the drone industry can enhance the safety and reliability of drone communications in the face of evolving threats.

2.4. Principles of Anti-Drone Defence

Regarding the increasing importance of defending against drones due to their potential malicious use, it also highlights the significance of cognitive radar systems in drone detection, stressing on advantages of speed and accuracy that cognitive radar has over traditional systems. The document also mentions a particular drone detection radar system made in South Korea that works under Ku-band with high-resolution signal processing technology capable of pinpointing drones precisely. This system integrates cognitive technology such

as Generative Adversarial Network (GAN) for real-time drone identification and detection.

Equally important, it describes what role antennas play in combating drones by explaining the differences between directional and omnidirectional antennas. For instance, Directional antennas work best when there is a need for long-distance signal transmission in one direction while Omnidirectional antennae transmit signals in all directions but within a short distance range. The paper suggests that directional antennas are best used on receivers to optimize signal reception from video transmitters whereas omnidirectional antennas are mostly associated with video transmitters to enable them to effectively adjust to changes in altitude and direction of the drone.

Moreover, it touches upon various communication protocols used in drones, providing a graphical overview of these protocols. It also references studies on the effectiveness of MaxWhere VR in spatial memory and mental rotation skills, as well as the integration of emotional display agents in virtual environments for usability evaluation. Additionally, the document mentions resources on pulse position modulation, quadcopter communication protocols, and the use of VR environments for cooperative learning. Overall, the PDF offers a comprehensive insight into the principles and technologies involved in anti-drone defence, highlighting the importance of cognitive radar systems and advanced signal processing techniques in countering drone threats.

2.5. Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies

The document talks about how the lack of reliable security protocols and the increasing number of heterogeneous connected devices makes Internet of Things (IoT) devices vulnerable to cyber-attacks. For instance, ethical hacking is vital in identifying weaknesses in IoT systems and coming up with mitigation strategies that can work against the anticipated risks. In another case of this sort, it becomes clear from the content that one must understand and address security vulnerabilities in IoT devices. The experiment involved capturing a legitimate controller device's MAC address, changing the MAC address of an attacking device to match, and successfully hijacking the drone thus illustrating the necessity for robust security measures within Io T environments.

Additionally, it stresses encryption as a critical measure for securing communications between controlling devices and such drones as existing in IoT. Continuous research and testing of security issues associated with various IoT devices using ethical hacking techniques are necessary to be a step ahead of possible cyber threats. There are also some strategies put forward by this paper on how to mitigate the damages caused by insecurity resulting from other future attacks made through drones or any other similar device under IoTs. By implementing effective security measures based on lessons learned from ethical hacking; organizations can improve their cybersecurity efforts

Overall, it underscores the critical role of ethical hacking in identifying vulnerabilities, testing security protocols, and developing robust mitigation strategies for IoT devices. With the increasing number of cyber-attacks on IoT devices, researchers and organizations need to stay vigilant, conduct thorough security assessments, and implement proactive measures to safeguard their IoT infrastructure. By addressing security challenges through ethical hacking practices and continuous research, the IoT ecosystem can enhance its resilience against evolving cyber threats and ensure the secure operation of connected devices.

2.6. Hacking a Commercial Drone with Open-Source Software: Exploring Data Privacy Violations

It shows how high the risks of violating data privacy are when drones are being used. The study designs its experiments around the de-authentication attack on a commercial drone to examine whether it is possible to compromise personal data, such as audio, video and location information. The research specifically targets one drone model as an example of how commercial drones are at risk and thus highlights the need for more efficient privacy legislations and policies for securing these machines.

The implications of this study include improving drone security measures, informing regulatory frameworks, and promoting industry standards to keep user data safe. Additionally, there is an opportunity for stakeholders to realize the importance of implementing strong security measures which include firmware updates, encryption protocols among others that will mitigate the risks

of unauthorized access and breach in data. This research also highlights how important it is to have privacy mechanisms like data encryption or secure authentication means so as not to violate any restrictions about privacy or permit any person's personal information stored on a commercial drone from leaking out.

Overall, the study contributes to advancing the understanding of drone security and privacy issues, prompting further research in the field to explore advanced attack techniques, countermeasures, and innovative solutions for addressing cybersecurity challenges in the drone industry. By applying the insights from this research, stakeholders can work towards creating a safer and more secure environment for drone users, ultimately enhancing the integrity of commercial drone operations and protecting user data from unauthorized access and exploitation.

2.7. Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA-based assessment

The paper explores cyber security issues related to using drones for monitoring critical infrastructure. It also points out some of the advantages of utilizing a fleet of drones like expanding mission capabilities through data transfer via intermediate nodes, increasing mission duration by replacing units with discharged batteries, enhancing system survivability in case of node failures through automatic network reconfiguration and reducing technical solution costs. It underscores the need to look at IoD architecture as cyber-physical systems where information forms its most reliable basis.

Additionally, this analysis details on IoD systems' network and information vulnerabilities noting that the network subsystem is more complicated and susceptible due to lack of determinism. It talks about how network architectures and mobile cloud technologies can be used to enable direct interaction among network devices using M2M architecture in self-organizing mobile networks. In addition, it identifies several cyber threats associated with IoD systems such as: gaining unauthorized access to resources over a computer network; manipulating operations within a computerized communication framework; taking charge over the entire system; modification in flow rules within network devices.

Moreover, it introduces the Intrusion Modes and Effects Criticality Analysis (IMECA) technique for assessing the cybersecurity properties of IoD networking. IMECA is applied to analyze the cyber vulnerabilities of IoD systems, categorizing potential attacks such as the imposition of false network routes, denial of service attacks, and remote launch of applications. The severity matrix generated through IMECA highlights the main danger to cybersecurity as man-in-the-middle attacks, especially for data and control channels established over the Internet. The document concludes by outlining future research directions and the need for continuous assessment and mitigation of cyber vulnerabilities in IoD systems.

2.8. Investigation of Drone Vulnerability and its Countermeasure

Drone vulnerability investigation and how to protect it indicated that drones are susceptible to wireless network attacks which underlines the importance of securing these gadgets. For example, Parrot AR Drone 2.0, DJI Spark, Parrot Disco FPV and DJI Robomaster S1, reveal security holes such as an open port and FTP access without a password. Therefore, images captured by DJI Spark drone are directly sent to the pilot's phone without being saved in the drone system; on the other hand, Parrot Disco FPV drone allows images through FTP at file path /Disco/media.

Both customers and vendors were given suggestions on how to enhance security. So, consumers were told to change their Wi-Fi hotspot name and passwords for unauthorized access prevention along with strong password recommendation as well as hiding SSID suggestions that could be used. On the other hand, firms were urged to institute some measures like stopping multi-connection among others in order to enhance these drones' safety precautions and adding Telnet and FTP passwords among others so that they can make your drones safer for you. MAC filtering is also a good way of controlling Wi-Fi connectivity while hidden SSID serves as a barrier against unauthorized connection from any one else who would want to control your drone.

In conclusion, the study compared the security levels of drones from different companies, noting that DJI drones appeared more secure than Parrot drones. The proposed countermeasures aimed to increase user awareness and protect against potential attacks, emphasizing the importance of securing drones'

wireless networks. By implementing these recommendations, both customers and vendors can mitigate the risks associated with drone vulnerabilities and enhance overall security measures in the drone industry.

3. DETAILS OF TECHNOLOGY

3.1. Kali Linux

Kali Linux is a Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security. The software is based on the Debian Testing branch: most packages Kali uses are imported from the Debian repositories.

Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber-attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), Metasploit (penetration testing framework), John the Ripper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners, etc.

It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix. The tagline of Kali Linux and BackTrack is “The quieter you become, the more you can hear”.

Kali Linux's popularity grew when it was featured in multiple episodes of the TV series Mr. Robot. Tools highlighted in the show and provided by Kali Linux include Bluesniff, Bluetooth Scanner (btscanner), John the Ripper, Metasploit Framework, Nmap, Shellshock, and Wget.

3.2. Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and analysis tool for 802.11 wireless LANs. It is used to assess the security of wireless networks. Aircrack-ng is commonly used by security professionals and ethical hackers to test the

vulnerabilities of wireless networks and to strengthen the security of these networks.

Here are some of the key components and functionalities of Aircrack-ng:

3.2.1. Airodump-ng

The tool is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vectors) for the intent of using them with aircrack-ng.

3.2.2. Aireplay-ng

It is used for packet injection. The primary purpose is to generate traffic for later use in aircrack-ng for cracking WEP and WPA-PSK keys.

3.2.3. Airmon-ng

This script enables and disables monitor mode on wireless interfaces. It is part of the aircrack-ng suite and is used to prepare the network interface for packet capturing.

3.2.4. Aircrack-ng

This is the main tool for cracking WEP and WPA/WPA2-PSK keys. It implements the standard FMS attack along with some optimizations like Korek attacks, as well as the PTW attack.

3.3. Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License version 2 or any later version.

Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

4. EXPERIMENTAL WORK

4.1. Airmon-ng

There are two modes of Network Interface Card (NIC). They are:

1. Managed Mode: By default, the mode of wireless devices is set to "Managed" which means our wireless device will only capture packets that have our device's MAC address as the destination MAC.
2. Monitor Mode: In Monitor mode, your card can listen to every packet that's around us.

This command is used for toggling the mode of the Network Interface Card (NIC). We need to set our NIC in “Monitor Mode” as by default it is in “Managed Mode”.

Command: airmon-ng start <interface>

Figure 1. Setting up wlan0 mode to Monitor.

4.2. Airodump-ng

Airodump-ng is used to list all the networks around us and display useful information about them. It is a packet sniffer, so it is designed to capture all the packets around us while we are in Monitor mode. We can run it against all of the networks around us and collect useful information like the Mac address, channel name, encryption type, and number of clients connected to the network

and then start targeting the target network. We can also run it against a certain AP (Access Point) so that we only capture packets from a certain Wi-Fi network.

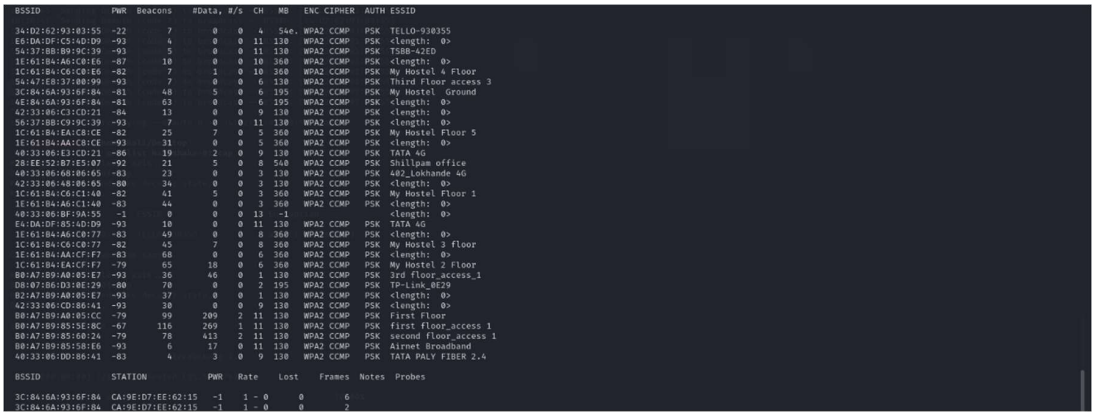

Figure 2. List all the networks around us along with information.

4.3. Aireplay-ng

The primary function is to generate traffic for later use in aircrack-ng for cracking the WEP and WPA-PSK keys. There are different attacks which can cause de-authentications for capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection.

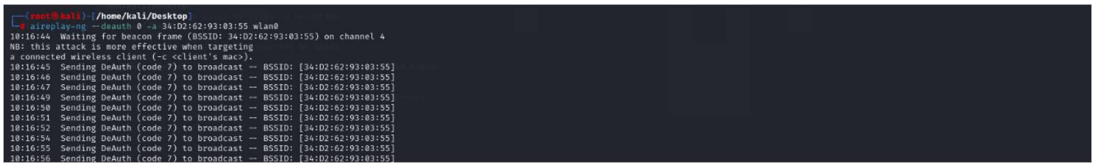

Figure 3. Sending de-authentication Packets to the target network.

4.4. Aircrack-ng

Using aircrack-ng involves providing the captured data (in .cap format) and specifying the attack parameters, such as the dictionary file or the key length for brute-force attacks. The tool will then analyze the captured data and attempt to recover the encryption key.

Figure 4. Analyzing the captured data and attempting to recover the encryption key.

AirCrack-ng will search the capture file for a match in the password list file. Once the key is found, it is displayed on the screen, along with how many keys were tested and the time it took to find the correct key.

4.5. Code Snippets

4.5.1. To Control Operations of Drone

```
import threading
import socket
import sys
import time

host = ''
port = 9000
locaddr = (host,port)

# Create a UDP socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
tello_address = ('192.168.10.1', 8889)
```

```
sock.bind(locaddr)

def recv():
    count = 0
    while True:
        try:
            data, server = sock.recvfrom(1518)
            print(data.decode(encoding="utf-8"))
        except Exception:
            print ('\nExit . . .\n')
            break

print ('\r\n\r\nTello Python3 Demo.\r\n')
```

```
print ('Tello: command takeoff land flip forward back
left right \r\n       up down cw ccw speed speed?\r\n')

print ('end -- quit demo.\r\n')

#recvThread create
recvThread = threading.Thread(target=recv)
recvThread.start()

while True:

    try:
        msg = input("");

        if not msg:
            break

        if 'end' in msg:
            print ('...')
            sock.close()
            break

        # Send data
        msg = msg.encode(encoding="utf-8")
        sent = sock.sendto(msg, tello_address)
    except KeyboardInterrupt:
        print ('\n . . .\n')
        sock.close()
        break
```

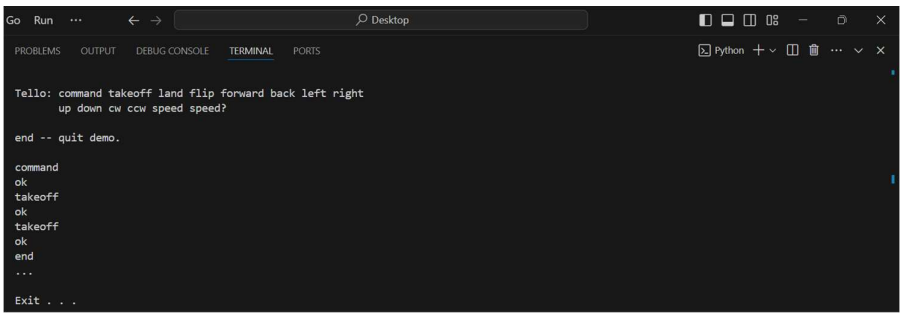

Figure 5. Controlling Drone through terminal

4.5.2. To Access the Drone Data

```
import socket
import keyboard
import cv2
```

```
import threading


def watch_video_stream(command_socket, command_addr):
    command_socket.sendto(b"streamon", command_addr)
    print("\n   video streaming started!")
    cap = cv2.VideoCapture('udp://192.168.10.1:11111')
    while True:
        ret, frame = cap.read()
        if ret:
            cv2.imshow('Tello Video Stream', frame)
            key = cv2.waitKey(1) & 0xFF
            if key == 27:  # 'Esc' key
                break
        else:
            break
    cap.release()
    cv2.destroyAllWindows()


def configure_wifi(command_socket, command_addr):

    ssid = input("\n   Enter new wifi SSID: ")
    print("   Done!")


def main():
    print("   Connect to Tello wifi and press <<Shift>>")
    while not keyboard.is_pressed("Shift"):
        pass
    print("   Starting")
    command_socket = socket.socket(socket.AF_INET,
socket.SOCK_DGRAM)
    command_addr = ('192.168.10.1', 8889)
    command_socket.bind(('', 8889))
    command_socket.sendto(b"command", command_addr)
    command_socket.recvfrom(1024)
    print("   Control has taken successfully!")
    video_thread =
threading.Thread(target=watch_video_stream,
args=(command_socket, command_addr))
    video_thread.daemon = True
    keyboard.on_press_key("1", lambda _:
command_socket.sendto(b"emergency", command_addr))
    keyboard.on_press_key("2", lambda _:
video_thread.start())
    keyboard.on_press_key("3", lambda _:
command_socket.sendto(b"land", command_addr))
```

```
    keyboard.on_press_key("4", lambda _:
configure_wifi(command_socket, command_addr))

    print("""
   press key for each function:
      1) Emergency - stop motors immediately
       2) Watch Video Stream
        3) Land
       4) Configure Wifi Password- lock the drone
      5) Exit
        """)
    while not keyboard.is_pressed("5"):
        pass


if __name__ == "__main__":
    main()
```

1. Drone Connected to mobile phone

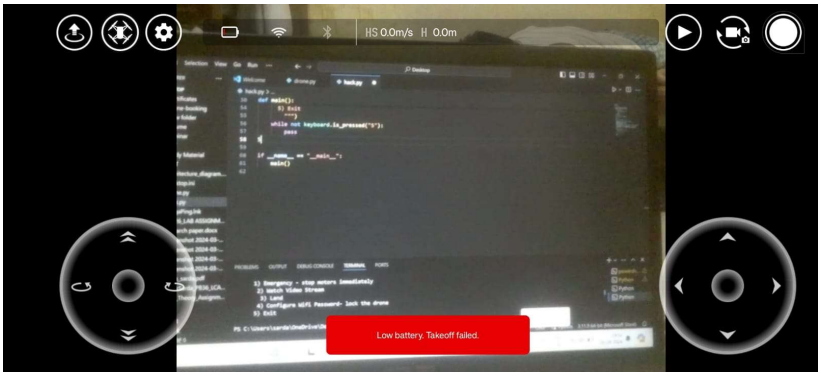

Figure 6. Drone connected to mobile phone

2. Successfully Disconnected to mobile phone

Figure 7. The drone got disconnected from the mobile phone

3. Successfully able to see the video stream

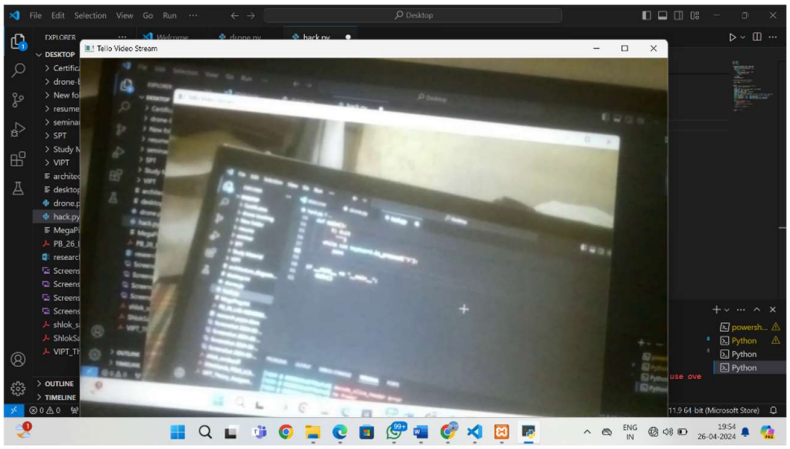

Figure 8. Video Stream of Drone

5. CONCLUSION

Through our experimental work, we found that commercial drones' Wi-Fi communication systems are vulnerable to various types of attacks. The de-authentication attacks and password-cracking methods we employed were successful in severing the connection between the drone and its pilot and potentially gaining unauthorized access to the drone's control.

These vulnerabilities highlight the critical need for improved security measures in commercial drones. Drone manufacturers should focus on implementing robust encryption protocols, secure authentication methods, and regular firmware updates to protect against such attacks.

Moreover, drone owners and operators should be educated about the importance of securing their Wi-Fi networks, such as using strong passwords, hiding SSIDs, and regularly updating their drone's firmware. Additionally, the adoption of advanced anti-drone systems and intrusion detection mechanisms can help in detecting and mitigating unauthorized drone activities.

In conclusion, while drones offer numerous benefits and applications across various sectors, their cybersecurity vulnerabilities pose significant risks. Continuous research, awareness, and proactive security measures are essential to ensure the safe and secure operation of drones in today's interconnected world.

6. FUTURE SCOPE

The research conducted on drone hijacking and its vulnerabilities offers a glimpse into the current state of drone security. As technology evolves, the drone industry is expected to grow exponentially, and so will the challenges related to drone security. Below are some potential areas for future research and development in this domain:

6.1. Advanced Encryption and Authentication Methods

One of the primary ways to enhance drone security is by implementing stronger encryption and authentication methods. Future research could focus on developing advanced encryption algorithms tailored for drone communication to prevent unauthorized access and data breaches.

6.2. AI and Machine Learning for Drone Security

Artificial Intelligence (AI) and Machine Learning (ML) can play a pivotal role in detecting anomalies and predicting potential security threats. Developing AI-driven security solutions that can learn from drone behaviour patterns and identify suspicious activities in real time could be a promising avenue for research.

6.3. Anti-Drone Technologies

With the increasing number of drones in the sky, the demand for anti-drone technologies will also rise. Future research could explore the development of more effective and affordable anti-drone systems capable of detecting, tracking, and neutralizing rogue drones without causing harm to legitimate ones.

6.4. Regulatory Framework and Policy Development

As drones become more integrated into our daily lives, there will be a need for comprehensive regulations and policies to govern their use and ensure public safety. Future research could focus on studying the existing regulatory frameworks and proposing new policies to address the security and privacy concerns associated with drones.

6.5. Ethical Hacking and Security Audits

Continued research in ethical hacking and security audits can help in identifying and addressing vulnerabilities in drone systems proactively. Organizing

hackathons and security challenges focused on drones can foster innovation and collaboration in the cybersecurity community.

6.6. Public Awareness and Education

Raising public awareness about the security risks associated with drones and educating drone owners and operators about best practices for securing their devices can play a crucial role in mitigating risks. Future initiatives could focus on developing educational programs, workshops, and awareness campaigns to promote drone security literacy.

6.7. Integration with Blockchain Technology

Blockchain technology offers decentralized and tamper-proof data storage, which can be beneficial for ensuring the integrity and security of drone data. Future research could explore the integration of blockchain technology with drone systems to enhance data protection and secure communication.

6.8. Collaboration with Industry Stakeholders

Collaboration between researchers, industry stakeholders, and government agencies is essential for addressing the complex challenges related to drone security. Future research initiatives could focus on fostering collaboration and knowledge-sharing platforms to facilitate the development of innovative solutions and best practices.

In conclusion, while the challenges related to drone security are significant, they also present opportunities for innovation and advancement. By focusing on these future research areas and collaborating across disciplines and sectors, we can work towards creating a safer and more secure environment for drone operations.

7. REFERENCES

1. R. Restituyo and T. Hayajneh, "Vulnerabilities and Attacks Analysis for Military and Commercial IoT Drones," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, pp. 26-32, doi: 10.1109/UEMCON.2018.8796596. keywords: {Vulnerabilities;Swarm;CIA;Exploits;Drones;RFcontrol},
2. K. Intwala, S. Jatav and K. Kolhe, "System to capture WiFi based Drones using IoT," 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA, Pune, India, 2022, pp. 1-6, doi: 10.1109/ICCUBEA54992.2022.10011038. keywords: {Wireless

communication;Wireless sensor networks;Smart cities;Software;Sensors;Internet of Things;Task analysis;Anti-drone System;IoT;Wireless Attacks;Automation},

3. M. Krichen, W. Y. H. Adoni, A. Mihoub, M. Y. Alzahrani and T. Nahhal, "Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures," 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 2022, pp. 184-189, doi: 10.1109/SMARTTECH54121.2022.00048. keywords: {Regulators;Face recognition;Employment;Machine learning;Mathematical models;Stakeholders;Software defined networking;Security;Drones;Communication;Attacks;Threats;Countermeasures;Blockchain;Machine Learning (ML);Fog Computing;Software Defined Network (SDN)},
4. P. Čisar, R. Pinter, S. M. Čisar and M. Gligorijević, "Principles of Anti-Drone Defense," 2020 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Mariehamn, Finland, 2020, pp. 000019-000026, doi: 10.1109/CogInfoCom50765.2020.9237841. keywords: {Airborne radar;Radar detection;Cognitive radar;Sensor systems;Kalman filters;Task analysis;Drones;anti-drone defense;radio modulation;remote control;antennas;spoofing;jamming;radar;hacking;cognitive detection},
5. G. Karmakar, M. Petty, H. Ahmed, R. Das and J. Kamruzzaman, "Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies," 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 2022, pp. 1-5, doi: 10.1109/CSDE56538.2022.10089255. keywords: {Ethics;Computer network reliability;Virtual machining;Internet of Things;Security;Reliability;Computer crime;Internet of Things;Ethical Hacking;Drone;Hijack;Mitigation Strategies},
6. J. Gabrielsson, J. Bugeja and B. Vogel, "Hacking a Commercial Drone with Open-Source Software: Exploring Data Privacy Violations," 2021 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2021, pp. 1-5, doi: 10.1109/MECO52532.2021.9460295. keywords: {Privacy;Data privacy;Embedded computing;Regulation;Computer crime;Open source software;Drones;Drone;UAV;Deauthentication;IoT;privacy;attack;open-source software},
7. V. Kharchenko and V. Torianyk, "Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, UKraine, 2018, pp. 364-369, doi: 10.1109/DESSERT.2018.8409160. keywords: {Drones;Monitoring;Cloud computing;Computer security;Data transfer;Network topology;Critical infrastructures;Unmanned Aerial Multisystems;Internet of Drones Cyber Vulnerabilities;Intrusion Modes and Effects Criticality Analysis},
8. N. Pojsomphong, V. Visoottiviseth, W. Sawangphol, A. Khurat, S. Kashihara and D. Fall, "Investigation of Drone Vulnerability and its Countermeasure,"

2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Malaysia, 2020, pp. 251-255, doi: 10.1109/ISCAIE47305.2020.9108835. keywords: {Drones;Unmanned Aerial Vehicle;Security Vulnerability;Penetration Testing},

9. https://www.statista.com/outlook/cmo/consumer-electronics/drones/india#analyst-opinion
10. https://sites.tufts.edu/eeseniordesignhandbook/files/2018/05/Real-Time-Transmission-of-Images-from-a-Drone-by-Ryan-Stocking.pdf