Use of AI Applications for the Drone Industry

Imdad Ali Shah
School of Computing Science, Taylor's University, Malaysia
shahsyedimdadali@gmail.com

NZ Jhanjhi
School of Computer Science, SCS Taylor's University, Malaysia
noorzaman.jhanjhi@taylors.edu.my

Raja Majid Ali Ujjan
School of Computing, Engineering & Physical Sciences Unversity of the West of Scotland
raja_majidali@hotmail.com

Abstract

The unmanned aerial vehicle (UAV) industry, commonly referred to as the drone industry, has grown rapidly in recent years and changed many industries' operational procedures. Drones are adaptable AUs that have the ability to operate independently or remotely. The drone business has developed into a vibrant, diverse sector with applications in many other industries. Drone technology is set to grow and become more integrated into daily life and corporate operations as long as regulations keep up with technological advancements. Artificial intelligence (AI) technologies are increasingly used in various industries, notably drone companies. AI can improve drone technology's effectiveness, dependability, and efficiency, creating new opportunities for the drone industry to service multiple applications and sectors. Applications of artificial intelligence (AI) have revolutionized a number of industries, but they have also raised serious privacy and security issues. In order to ensure ethical and responsible AI deployment, it is imperative to comprehend and solve these concerns as AI systems become more complex and ubiquitous. Recent scientific and technical developments have resulted in constant advances in aircraft manufacturing and the information industry, resulting in new technologies, materials, and production methods. The technical makeup of UAV systems has been drastically altered because of the incorporation and use of these technological breakthroughs. The UAV business may expand quickly and become a primarily independent sector because IT has permeated the aviation sector. Drone and AI technologies have the potential to revolutionize a wide range of fields and applications. The complexity of the software and technology in UAVs also raises privacy and security concerns and poses significant challenges for organizations in the private and public sectors. The drone can send and receive information in the communication system, such as transmitter orders or sensor monitoring data. Wi-Fi, Bluetooth, and cellular networks are just some options for accomplishing this. Since several security flaws might affect these UAVs, they are constantly under attack. The primary object of this chapter is to evaluate the AI applications for the drone Industry and identify privacy and security issues and challenges. Our result will help the next generation and open doors for new researchers.

Keywords: AI Applications, UAV systems, Drone Industry, Security issues, and challenges

1. Introduction

A new age of innovation and opportunities has begun due to the advent of artificial intelligence (AI) applications in the drone sector. Drones are becoming more versatile, practical, and adaptable to different industries thanks to the use of AI to improve their capabilities and functionalities. Incorporating AI into the drone industry improves the capabilities of these unmanned aerial vehicles while also creating new business prospects across several industries. We may anticipate increasingly advanced and intelligent drone uses as AI develops, further transforming industries and enhancing our daily lives A. Fotouhi, 2019. Unmanned aerial vehicles (UAVs), drones, can be flown autonomously by aircraft computers or remotely by people. UAVs operate similarly to airplanes in that they can lift themselves using aerodynamic principles and transport objects like cameras, weapons, and other items. Drones were initially developed and utilized by the military to strike adversaries. In general, this drone's initial application is in the military A. Chriki, 2019, A. I. Hentati, 2020. However, it can be applied invarious industries because of the shifting times. Figure 1 Overview of drone applications.

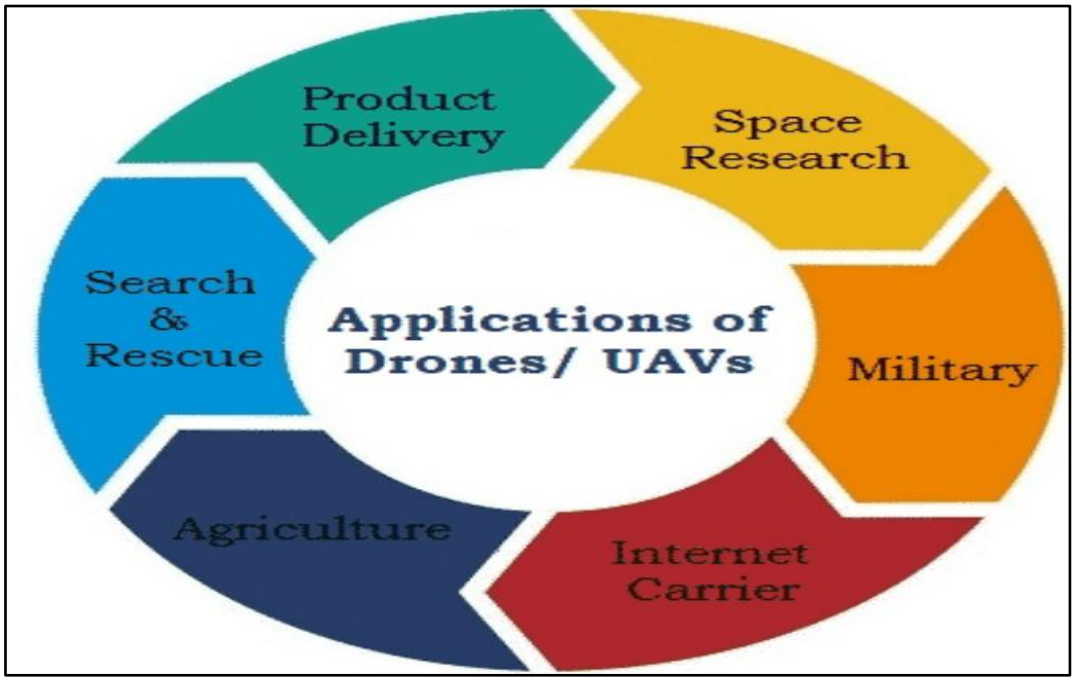

Fig 1 *Overview of drone applications adopated from cfdflowengineering.com*

Particularly in the IoT era, artificial intelligence technology is developing at a rapid rate. Drones and artificial intelligence make for attractive technological partners. Artificial AI is a computer program that can simulate human intelligence, including decision-making, problem-solving, and prediction A. Sharma, 2020, A. Shafique, 2021. The function of the drone is made more sophisticated by the addition of artificial intelligence so that it can assist people with challenging tasks. As an industrial nation, Indonesia was added to the list in 2017 (Kemenperin). Indonesia, a developing country with an industrial base, unquestionably requires new technology to support and advance the sector. With the development of industrial drone technology, it is anticipated that drone applications will be able to outcompete big businesses globally A. Koubaa, 2019. The Indonesian government supports the use of drones in various government initiatives. The government also controls how drones are used. Drones can be used for various activities, including infrastructure monitoring, cargo delivery. Drones can fly, which allows them to ship things more swiftly and effectively. A drone acting as a

firefighting forest can assist in putting out burned forests, particularly inaccessible forest areas, and can also protect firefighters A. K. Sikder, 2021. The drone explores mining materials and records photographs that track the growth of the mining region.

This Chapter will focus on the following points:-

1. This chapter focuses on the drone Industry.
2. This chapter focuses on drone data security.
3. This chapter focuses on the Privacy and Security Issues Using AI Applications.
4. This chapter focuses on drone privacy issues
5. This chapter provides future recommendations.

2. Literature Review

Unmanned aerial vehicle (UAV) capabilities and functionality have been improved in various ways thanks to applications of artificial intelligence (AI) that have had a significant impact on the drone industry. Drones are becoming increasingly capable, effective, and adaptable in their functions across numerous sectors as AI technology progresses B. Nassi, 2019, Balakrishnan, 2023. The legislation lists some places where flying drones are prohibited but leaves out the areas where they are permitted. The law states that drone activities at heights more than 500 feet (150 m) are only allowed if the Director General of Civil Aviation approves them following receipt of a referral from the appropriate institution in the region or airspace. As a result, Indonesian drone usage must adhere to and comply with all applicable laws. The oil palm plantation industry in Indonesia was the first to employ drones for industrial purposes. Drones are frequently employed in the plantation sector to gather up-to-the-minute data on the state of oil palm plants B. Nassi, 2021. By collecting photographs of vast plantations, drones are used for routine operational tasks. The plantation business believes that using these drones is practicable and cost-effective enough to provide knowledge for management to measure the success of crop management precisely.

Drones are now often employed for civil purposes because of technological advancements, particularly in commerce, industry, and logistics. Infrastructure, oil and gas, agriculture, and construction sectors have started considering drone technology as a possibility. Because Indonesia has a lot of agricultural land and is developing its infrastructure on its territory, the infrastructure and agriculture sectors need drone technology C. G. Krishna, 2017, M. Y. Arafat, 2019. Drone technology was chosen because it can enhance business performance, particularly in decision-making. Additionally, the industry will gain insight into the prospects for drone applications in business thanks to the availability of drones at reasonably low prices. Drones were initially created for military use in the early 1900s as a component of weapons to strike an adversary. This pilotless aircraft flies at specific periods and then dumps torpedo bombs on a target. However, because of its accuracy rate, it cannot be used in actual warfare operations. The drone is still being developed, though Chhajed, 2022,. Then, the military developed unmanned aerial vehicles (UAVs), where Israel and the United States created additional capabilities, including espionage and monitoring. An overview of data security is in Figure 2.

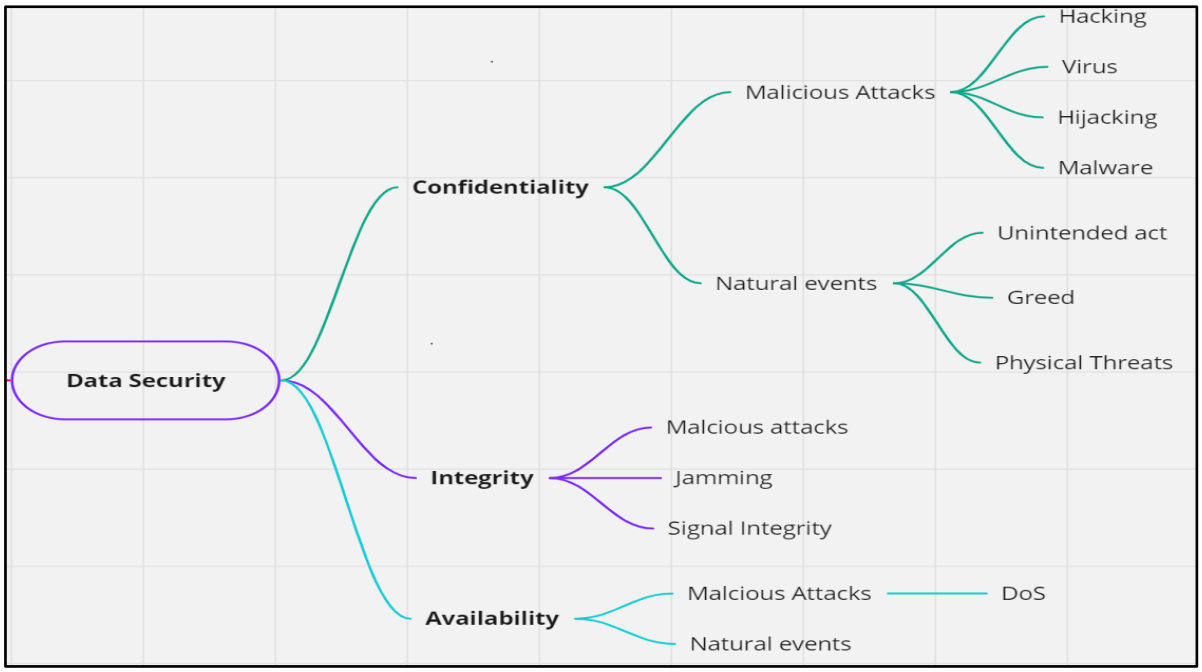

Fig 2 *Overview of data security*

Many military analysts predict that this drone will be the center of military power in the future (Um, 2019). Unmanned aerial vehicles have been developed recently in several nations, including Indonesia, due to their recognition of their utility and necessity. The previous several drones have been enhanced for civilian and military uses C. Lin, 2018, M. Yahuza,2021. Drone technology for photography has developed because there is a societal need for it. Drone photography can be seen as a toy that can be played with, but the operation is complex, and the pictures tremble. Since then, there has been progress due to the quick advancement of drone shooting technology, including gimbals to absorb shocks during filming and video transmission and receiver devices. The shooting era is currently flourishing. Additionally, more robust software is available to operate drones, allowing them to fly steadily and to the desired place. D. Mishra , 2020, M. Varshosaz,2019 Large datasets are frequently necessary for AI to function well, and the gathering, storing, and processing of personal data raises serious privacy issues. The analysis of user behavior and preferences by AI algorithms raises concerns regarding user data handling, access controls, and potential misuse. D. Shumeye Lakew, 2020, N. A. Khan,2020 Applications using AI are not safe from online attacks. Because AI systems handle enormous volumes of data, bad actors find them to be appealing targets. Security flaws may allow for unauthorized control or manipulation of AI systems in certain situations, compromise private data, and result in data breaches.

3. Drones Industry

The unmanned aerial vehicle (UAV) industry, commonly referred to as the drone industry, has grown rapidly in recent years and changed many industries' operational procedures. Drones are adaptable aerial vehicles that have the ability to operate independently or remotely. It takes a multipronged strategy combining technology, legislation, and public awareness to address these security issues. Governments, businesses, and tech companies are putting a lot of effort into coming up with ways to keep drone operations safer while maintaining their useful uses. The drone business has grown and diversified significantly, providing a range of uses in industries like filmmaking, delivery, monitoring, and agriculture Dawson, M., 2022, N. Iqtidar,2021. Drones have many advantages, but they also present unique security risks.

Unmanned aerial vehicles are becoming more common among business users and enthusiasts. In addition, they are employed in farming for agricultural upkeep, in law enforcement for surveillance, in monitoring the poaching of wild animals in Africa, and in obtaining specialized movie and sporting event footage F. Noor, 2020, F. Syed, 2021. Additionally, there have been instances of the technology being employed for evil intent, including physical attacks, intrusions into secure locations, including the UK Parliament, royal palaces, the White House, and prisons, and interference with civil aviation. There is a growing need for forensic examination of these devices due to the popularity of drones and their potential use for criminal activity.

Unmanned aerial vehicles (UAVs) have made a variety of tasks and industries easier to complete. Higher levels of dependability and more reassuring levels of trust in the employment of UAVs in the air have been made possible by integrating the most recent technologies Additionally, drones can detect impediments in real-time, identify them, and avoid potential collisions G. Choudhary, 2018, Gaur, L., 2018, Shah, I. A.,2024. A drone without computer vision can take digital pictures and movies of its surroundings; it cannot comprehend and engage with them.

A thorough forensic analysis of a drone will consider all available evidence, including DNA and fingerprints, which may help determine the rightful owner of the object and provide a line of inquiry that, among other advantages, can help locate further sources of evidence. The drone device should be turned off when secured to avoid the data being compromised G. Choudhary, 2018, H. Sedjelmaci, 2016. It is reasonable to anticipate that as drones' use for illicit purposes grows, so will the variety of drone makers and types available on the market. As a result, the issues faced in mobile forensics, a growing variety of devices and operating systems that examiners will expect to encounter, are expected to present themselves and be akin to those faced in studying the spectrum of drones that become involved with criminal activity. The study of drones is anticipated to benefit from additional data collection techniques like JTAG and chip-off. The unmanned aerial vehicle (UAV) sector, commonly called the drone industry, has experienced substantial growth and development in recent years. Drones are aircraft that can be operated remotely or autonomously without a human pilot present. They are used in a variety of industries and fields H. Shakhatreh, 2019, Hussain, M., 2022, Shah, I. A., Jhanjhi, 2024. The drone industry is vibrant and changing quickly, with many potentials and difficulties. Drones are anticipated to become more integral to various industries as technology develops, and rules change to reflect the environment. Figure 3 Overview of the drone Industry's primary components.

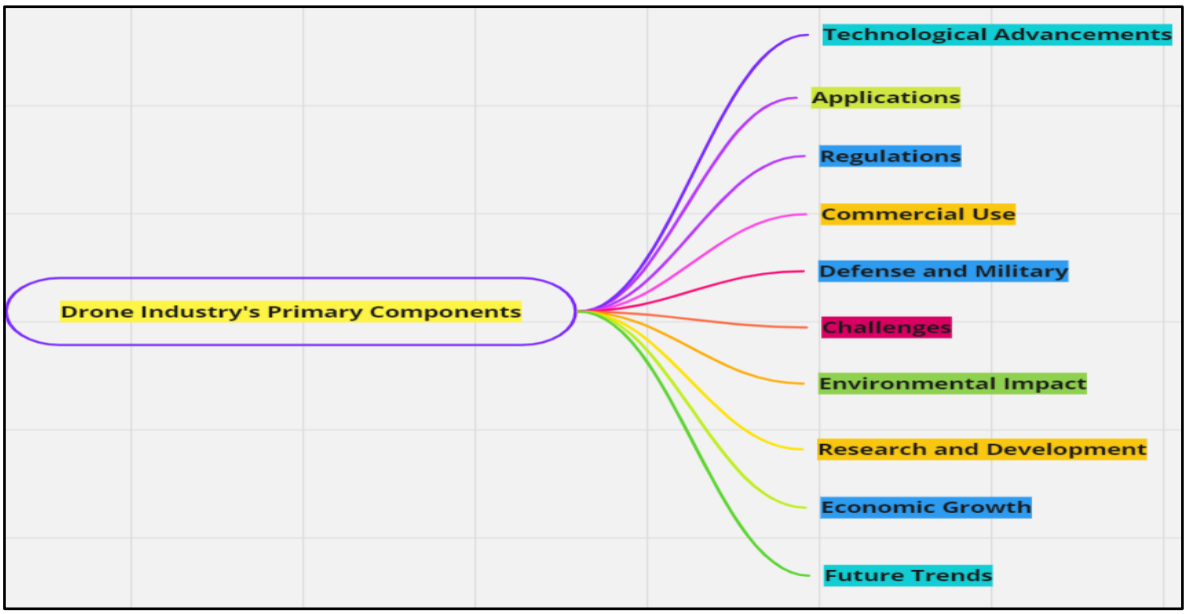

Fig 4 *Overview of drone Industry's primary components*

3.1 Applications

Agriculture, building, infrastructure inspection, environmental monitoring, cinematography, search and rescue, delivery services, military and defense, and recreational use are just a few businesses that use drones Jhanjhi, N. Z., 2022, N. Hossein Motlagh, 2016. They can conduct jobs, access dangerous or difficult-to-reach regions, and collect data.

3.2 Technological Advancements

Technology has advanced quickly in the drone sector. Drones are becoming more capable and affordable thanks to advances in battery life, compact and potent sensors, and data processing O. S. Oubbati, 2019. Drones have been equipped with AI and machine learning to increase their autonomy.

3.3 Regulations

To ensure the safe and responsible use of drones, governments and aviation authorities all over the world have put restrictions in place. These rules encompass things like operator licensing, flight limitations, and registration. Both business and recreational drone operators must abide by these regulations.

3.4 Commercial Use

Drone-related commercial uses are increasing. Businesses are turning to drones for jobs like aerial photography, surveying, crop monitoring, and infrastructure inspection P. Boccadoro, 2020. Drone delivery solutions are being investigated by delivery firms, particularly in the e-commerce industry.

3.5 Defense and Military

Modern military and defense activities now rely heavily on drones. They are employed in offensive operations as well as observation and surveillance R. Kellermann, 2020. Several nations have created and used armed drones, also called UAVs.

4. Challenges

The drone industry confronts security, privacy, and safety difficulties. Continuous challenges include protecting private information, preventing unauthorized drone use, and ensuring that drones do not interfere with manned aircraft. Counter-drone equipment has also been created to counter possible risks from malicious drone operators.

4.1 Environmental Impact

Drones hurt the environment, particularly in terms of energy use and emissions. Drone technology developers are aiming to create more environmentally friendly drones.

4.2 Research and Development

The drone industry's ongoing research and development pushes the limits of what drones are capable of. This includes materials, automation, energy sources, and propulsion systems advancements.

4.3 Economic Growth

In several nations, the drone business has helped the economy flourish. Jobs in drone-related manufacturing, maintenance, software development, and data analysis have been made possible. Artificial intelligence (AI) has made great strides in recent years and is currently utilized in various fields and applications. Healthcare, finance, education, customer service, retail, manufacturing, transportation, security, and marketing are some of the most notable AI applications now being used R. Guo, 2020,. Figure 5 Overview of AI applications: there are several AI applications.

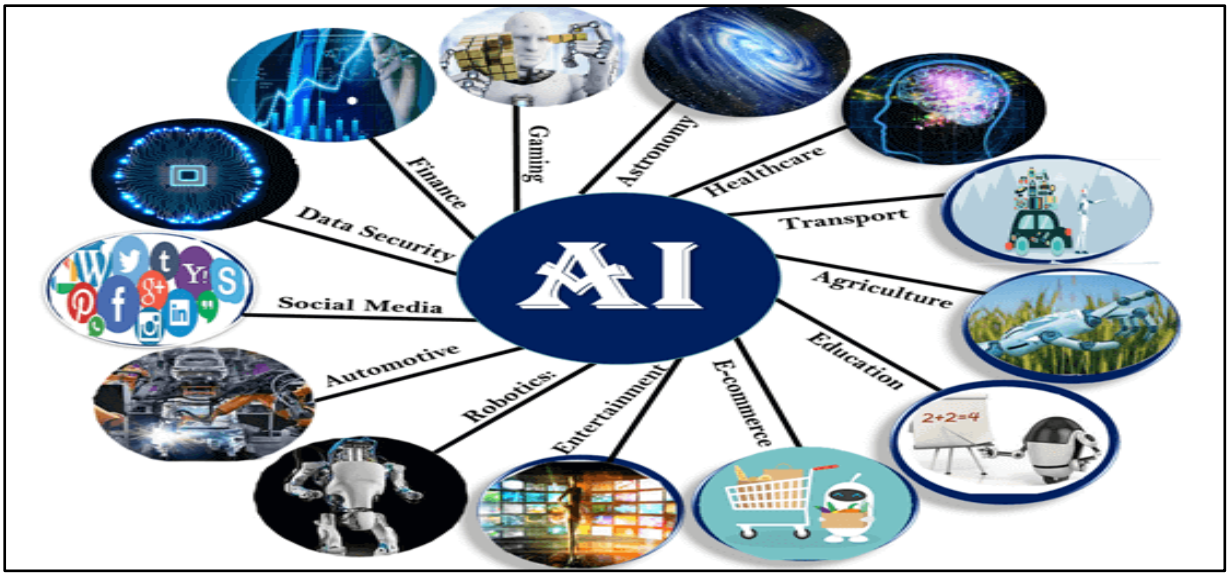

Figure 5 Overview of AI applications adopated from javatpoint.com

5. Privacy and Security Issues Using AI Applications

For AI systems to work well, a lot of data is frequently needed. Concerns around data usage, access, and retention periods are brought up by the gathering and storage of personal information. J.-P. Yaacoub,2020, Shah, I. A.,2022. Users might not always be completely aware of how much AI applications are using their data. It becomes difficult to get informed permission, particularly when data is being gathered for uses other than those for which consumers first consented. J. Aru Saputro, 2020, Shah, I. A.,2022 Hackers are drawn to AI systems because of the vast volumes of data they hold. Sensitive personal data may become public due to a breach, which could have dangerous repercussions for individuals. Kiran, S. R. A., 2021, Shah, I. A., 2023, additionally susceptible to hacker attempts that alter or impair their operation are artificial intelligence (AI) systems. Adversarial attacks, for instance, entail providing false information on purpose in order to trick the AI system. It takes a multifaceted strategy including technology developers, policymakers, and users to address these privacy and security challenges. It entails putting strong security measures in place, encouraging openness, and creating moral standards for the creation and use of AI applications.

An array of privacy and security issues have arisen as a result of the growing incorporation of artificial intelligence (AI) into diverse applications. It is crucial to strike a careful balance between innovation and protecting individual rights as AI systems become more complex and widespread. L. Watkins, 2021, Umrani, S., 2020, Inadequate security measures during the gathering and processing of personal data may result in privacy violations. People might not be aware of how much of their data is being utilized, which raises questions about their ability to give informed permission. L. P. Rondon, 2021, Ujjan, R. M. A.,2018, AI-driven surveillance systems have the potential to compromise individual privacy, especially those that use facial recognition software. AI systems are vulnerable to various cyber threats, including data breaches, ransomware attacks, and manipulation of AI models. Compromised systems can lead to unauthorized access to sensitive information. Adversarial attacks involve manipulating input data to deceive AI models. Ensuring the robustness of AI models against such attacks is a significant security challenge. Vulnerabilities in the model can be exploited to produce incorrect or harmful outputs. Ujjan, R. M. A.,2020, Z. Li,2019. Corrupted data may arise from manipulating the training data. Artificial intelligence systems may make inaccurate predictions or choices as a result of deliberate or inadvertent data poisoning during the training process. Applications using AI frequently rely on external libraries, parts, and services. For the AI system to be secure overall, these components' security is essential Ujjan, 2022, Ujjan, R.M.A.,2022, Y. M. Kwon,2018. The integrity and security of the AI application can be jeopardized by taking advantage of any weaknesses in the supply chain. While there are many advantages to the widespread use of AI technologies, there are also serious privacy and security concerns. A comprehensive strategy incorporating not only scientific break throughs but also ethical concerns and strong legal frameworks is needed to strike a balance between the benefits of artificial intelligence and the protection of individual rights. Fig 6 Overview Privacy issues of drones.

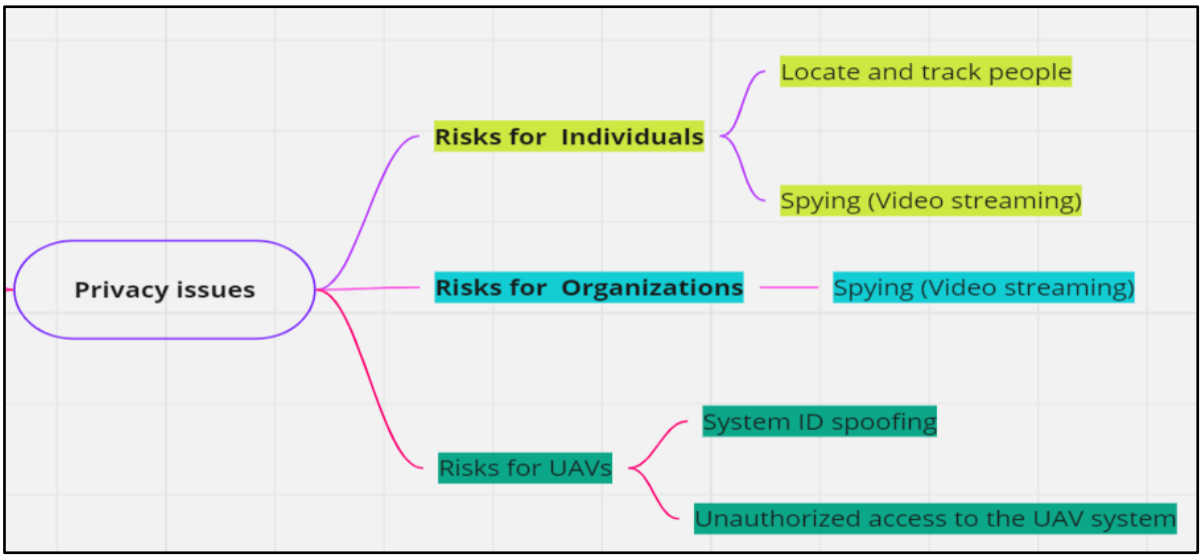

Fig 7 *Overview Privacy issues of drones*

UAV network security and privacy concerns from the standpoint of the cyber-physical system (CPS). Ujjan, R. M. A., Taj, I.,2022 investigated the shortcomings of the security measures employed by UAVs, and reviewed the state-of-the-art technology used in the literature to solve privacy and security concerns with UAVs. The writers looked into concerns related to safety, privacy, and security for commercial drones. They specifically noted the drone's primary vulnerabilities, including cyber and physical threats and potential attack vectors that may lead to a crash during a flight operation. Similarly, the authors investigated the issues and emerging cyber threats that commercial drones must contend with M. Mozaffari, 2019, V. Hassija,2021. Examined the risks and questionable civilian use of drone technology. In their most recent study, carried out a detailed survey of the literature on security and privacy problems related to commercial drones. investigated the serious security issues surrounding UAV-supported cellular communications. In a different study, Y. Zhi, Z. Fu,2020, looked into the privacy and security risks associated with UAV network design. Ad hoc communication among several UAVs is one of the biggest challenges. The possibility of both passive and aggressive attacks is significantly increased when UAVs are present in the national airspace due to security concerns. Figure 6 Overview of privacy issues of drones.

Chapter Contribution and Recommendations

The primary object of this chapter is to evaluate the AI applications for the drone Industry and identify privacy and security issues and challenges. Drone technology is set to grow and become more integrated into daily life and corporate operations as long as regulations keep up with technological advancements. Artificial intelligence (AI) technologies are increasingly used in various industries, notably drone companies. AI can improve drone technology's effectiveness, dependability, and efficiency, creating new opportunities for the drone industry to service multiple applications and sectors. Applications of artificial intelligence (AI) have revolutionized several industries, but they have also raised serious privacy and security issues. To ensure ethical and responsible AI deployment, it is imperative to comprehend and solve these concerns as AI systems become more complex and ubiquitous. Recent scientific and technical developments have resulted in constant advances in aircraft manufacturing and the information industry, resulting in new technologies, materials, and production methods. The technical makeup of UAV systems has been drastically altered because of the incorporation and use of these technological breakthroughs. The UAV business may expand quickly and

become a primarily independent sector because IT has permeated the aviation sector. Drone and AI technologies have the potential to revolutionize a wide range of fields and applications. While the current countermeasures aim to address security concerns, UAVs can violate personal privacy by acquiring sensitive information about organizations or by eavesdropping on people's daily activities. Without clear restrictions, using UAVs in civilian airspace raises major privacy problems for people. Additionally, UAV-collected sensitive data sent to the GCS must be secured from outside interference.

For AI systems to work well, a lot of data is frequently needed. Concerns around data usage, access, and retention periods are brought up by the gathering and storage of personal information. Users might not always be completely aware of how much AI applications are using their data. It becomes difficult to get informed permission, particularly when data is being gathered for uses other than those for which consumers first consented. Hackers are drawn to AI systems because of the vast volumes of data they hold. Sensitive personal data may become public due to a breach, which could have dangerous repercussions for individuals. Additionally susceptible to hacker attempts that alter or impair their operation are artificial intelligence (AI) systems. Adversarial attacks, for instance, entail providing false information on purpose in order to trick the AI system. It takes a multifaceted strategy including technology developers, policymakers, and users to address these privacy and security challenges. It entails putting strong security measures in place, encouraging openness, and creating moral standards for the creation and use of AI applications.

It's critical to address these privacy and security concerns as AI develops. Collaboration between technologists, legislators, ethicists, and legal experts across other disciplines is necessary to strike a balance between innovation and protecting individual rights. By means of thorough investigation, conscientious development methodologies, and well-considered legislation, the advantages of artificial intelligence can be leveraged while minimizing the prospective hazards to confidentiality and safety.

6. Conclusion

We provided a thorough analysis of the privacy and security concerns pertaining to unmanned aerial vehicles. At the sensor, hardware, software, and communication levels—the four levels of UAV security—we thoroughly examined the concerns. We also talked about the risks associated with UAV privacy and potential remedies. We then discussed the security and privacy implications of UAVs, outlining the lessons we had learned and suggesting potential avenues for further research. The growing quantity of commercial unmanned aerial vehicles (UAVs) operating in public airspace has made security and privacy concerns a critical national security issue. Therefore, new security frameworks, standards, and laws need to be developed in partnership with industry, academia, and law enforcement. Security and privacy concerns must keep up with the next generation of commercial UAVs being introduced to the market by established drone manufacturers.

7. Future work

It's critical to address these privacy and security concerns as AI develops. Collaboration between technologists, legislators, ethicists, and legal experts across other disciplines is necessary to strike a balance between innovation and protecting individual rights. By means of thorough investigation, conscientious development methodologies, and well-considered legislation, the advantages of artificial intelligence can be leveraged while minimizing the

prospective hazards to confidentiality and safety. Consequentially, collaboration between business, academics, and law enforcement is required to create new security frameworks, standards, and legislation. As reputable drone manufacturers release the next generation of commercial UAVs onto the market, security and privacy concerns need to keep up.

References

A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. GarciaRodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3417–3442, 2019.

A. I. Hentati and L. C. Fourati, "Comprehensive survey of UAVs communication networks," Computer Standards and Interfaces, vol. 72, no. September 2019, p. 103451, 2020.

A. Sharma, P. Vanjani, N. Paliwal, C. M. Basnayaka, D. N. K. Jayakody, H. C. Wang, and P. Muthuchidambaranathan, "Communication and networking technologies for UAVs: A survey," Journal of Network and Computer Applications, vol. 168, no. June, p. 102739, 2020.

A. Shafique, A. Mehmood, and M. Elhadef, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles," IEEE Access, vol. 9, pp. 46 927–46 948, 2021.

A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "UAV-GCS centralized data-oriented communication architecture for crowd surveillance applications," in 2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019, 2019, pp. 2064–2069.

cfdflowengineering.com, https://cfdflowengineering.com/classification-and-application-of-drones/

A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," IEEE Access, vol. 7, pp. 87 658–87 680, 2019.

A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications," IEEE Communications Surveys and Tutorials, vol. 23, no. 2, pp. 1125–1159, 4 2021.

B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "SoK - Security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps," arXiv, pp. 1–17, 2019. [Online]. Available: http://arxiv.org/abs/1903.05155

B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and Privacy in the Age of Commercial Drones," 2021 2021 IEEE Symposium on Security and Privacy (SP), no. Section IV, pp. 73–90, 2021.

Balakrishnan, S., Ruskhan, B., Zhen, L. W., Huang, T. S., Soong, W. T. Y., & Shah, I. A. (2023). Down2Park: Finding New Ways to Park. *Journal of Survey in Fisheries Sciences*, 322-338.

C. G. Krishna and R. R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” SSRR 2017 - 15th IEEE International Symposium on Safety, Security and Rescue Robotics, Conference, pp. 194–199, 2017.

Chhajed, G. J., & Garg, B. R. (2022). Applying Decision Tree for Hiding Data in Binary Images for Secure and Secret Information Flow. In *Cybersecurity Measures for E-Government Frameworks* (pp. 175-186). IGI Global.

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.

D. Mishra and E. Natalizio, “A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements,” Computer Networks, vol. 182, no. August, p. 107451, 2020.

D. Shumeye Lakew, U. Sa’Ad, N. N. Dao, W. Na, and S. Cho, “Routing in Flying Ad Hoc Networks: A Comprehensive Survey,” IEEE Communications Surveys and Tutorials, vol. 22, no. 2, pp. 1071–1120, 4 2020.

Dawson, M., & Walker, D. (2022). Argument for Improved Security in Local Governments Within the Economic Community of West African States. *Cybersecurity Measures for E-Government Frameworks*, 96-106.

F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, “A review on communications perspective of flying AD-HOC networks: Key enabling wireless technologies, applications, challenges and open research topics,” Drones, vol. 4, no. 4, pp. 1–14, 2020.

F. Syed, S. K. Gupta, S. Hamood Alsamhi, M. Rashid, and X. Liu, “A survey on recent optimal techniques for securing unmanned aerial vehicles applications,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 7, 2021.

G. Choudhary, V. Sharma, I. You, K. Yim, I. R. Chen, and J. H. Cho, “Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey,” 2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018, pp. 560–565, 2018.

Gaur, L., Ujjan, R. M. A., & Hussain, M. (2022). The Influence of Deep Learning in Detecting Cyber Attacks on E-Government Applications. In *Cybersecurity Measures for E-Government Frameworks* (pp. 107-122). IGI Global.

G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, “Internet of drones (IoD): Threats, vulnerability, and security perspectives,” in The 3rd International Symposium on Mobile Internet Security, no. 37, 2018, pp. 1–13.

H. Sedjelmaci, S. M. Senouci, and M. A. Messous, “How to detect cyber-attacks in unmanned aerial vehicles network?” 2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings, 2016.

H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, “Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges,” IEEE Access, vol. 7, pp. 48 572–48 634, 2019.

Hussain, M., Talpur, M. S. H., & Humayun, M. (2022). The Consequences of Integrity Attacks on E-Governance: Privacy and Security Violation. In *Cybersecurity Measures for E-Government Frameworks* (pp. 141-156). IGI Global.

Jhanjhi, N. Z., Ahmad, M., Khan, M. A., & Hussain, M. (2022). The impact of cyber attacks on e-governance during the covid-19 pandemic. In *Cybersecurity Measures for E-Government Frameworks* (pp. 123-140). IGI Global.

J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” Internet of Things, vol. 11, p. 100218, 2020.

javatpoint.com, https://www.javatpoint.com/application-of-ai

J. Aru Saputro, E. Egistian Hartadi, and M. Syahral, “Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test,” Proceeding - 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering, ICITAMEE 2020, pp. 95–100, 10 2020.

Kiran, S. R. A., Rajper, S., Shaikh, R. A., Shah, I. A., & Danwar, S. H. (2021). Categorization of CVE Based on Vulnerability Software By Using Machine Learning Techniques. *International Journal*, *10*(3).

L. Watkins, J. Ramos, G. Snow, J. Vallejo, W. H. Robinson, A. D. Rubin, J. Ciocco, F. Jedrzejewski, J. Liu, and C. Li, “Exploiting multivendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems,” Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, Mobile IoT SSP 2018, 2018.

L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, “Survey on Enterprise Internet-of-Things Systems (EIoT): A Security Perspective,” 2021. [Online]. Available: http: //arxiv.org/abs/2102.10695

L. Gupta, R. Jain, and G. Vaszkun, “Survey of Important Issues in UAV Communication Networks,” IEEE Communications Surveys and Tutorials, vol. 18, no. 2, pp. 1123–1152, 2016.

M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, “Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges,” IEEE Access, vol. 9, pp. 57 243–57 270, 2021.

M. Mozaffari, W. Saad, M. Bennis, Y. H. Nam, and M. M. Debbah, “A tutorial on UAVs for wireless networks: Applications, challenges, and open problems,” IEEE Communications Surveys and Tutorials, vol. 21, no. 3, pp. 2334–2360, 2019.

M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, and E. G. Parmehr, “Spoofing detection of civilian UAVs using visual odometry,” ISPRS International Journal of Geo-Information, vol. 9, no. 1, 2019.

N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, and A. Nayyar, “Emerging use of UAV’s: secure communication protocol issues and challenges,” in Drones in Smart-Cities. Elsevier Inc., 2020, pp. 37–55.

N. Iqtidar, S. Kumar, R. Ashiqur, and U. Selcuk, “A Survey on Security and Privacy Issues in Modern Healthcare Systems,” ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 1–44, 7 2021.

N. Hossein Motlagh, T. Taleb, and O. Arouk, “Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 899–922, 2016.

O. S. Oubbati, M. Atiquzzaman, P. Lorenz, M. H. Tareque, and M. S. Hossain, “Routing in flying Ad Hoc networks: Survey, constraints, and future challenge perspectives,” IEEE Access, vol. 7, pp. 81 057–81 105, 2019.

P. Boccadoro, D. Striccoli, and L. A. Grieco, “An Extensive Survey on the Internet of Drones,” Tech. Rep., 2020. [Online]. Available: http://arxiv.org/abs/2007.12611

R. Kellermann, T. Biehle, and L. Fischer, “Drones for parcel and passenger transportation: A literature review,” Transportation Research Interdisciplinary Perspectives, vol. 4, p. 100088, 3 2020.

R. Guo, B. Wang, and J. Weng, “Vulnerabilities and Attacks of UAV Cyber Physical Systems,” ACM International Conference Proceeding Series, pp. 8–12, 2020.

Shah, I. A., Wassan, S., & Usmani, M. H. (2022). E-Government Security and Privacy Issues: Challenges and Preventive Approaches. In *Cybersecurity Measures for E-Government Frameworks* (pp. 61-76). IGI Global.

(2022). Cybersecurity Issues and Challenges for E-Government During COVID-19: A Review. *Cybersecurity Measures for E-Government Frameworks*, 187-222.

Shah, I. A., Habeeb, R. A. A., Rajper, S., & Laraib, A. (2022). The Influence of Cybersecurity Attacks on E-Governance. In *Cybersecurity Measures for E-Government Frameworks* (pp. 77-95). IGI Global.

Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2023). Cybersecurity and Blockchain Usage in Contemporary Business. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (pp. 49-64). IGI Global.

Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Enabling Explainable AI in Cybersecurity Solutions. In *Advances in Explainable AI Applications for Smart Cities* (pp. 255-275). IGI Global.

Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Artificial Intelligence Applications in the Context of the Security Framework for the Logistics Industry. In *Advances in Explainable AI Applications for Smart Cities* (pp. 297-316). IGI Global.

Umrani, S., Rajper, S., Talpur, S. H., Shah, I. A., & Shujrah, A. (2020). Games based learning: A case of learning Physics using Angry Birds. *Indian Journal of Science and Technology*, *13*(36), 3778-3784.

Ujjan, R. M. A., Pervez, Z., & Dahal, K. (2018, June). Suspicious traffic detection in SDN with collaborative techniques of snort and deep neural networks. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 915-920). IEEE.

Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., & González, J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. *Future Generation Computer Systems*, *111*, 763-779.

Ujjan, Raja Majid Ali, Imran Taj, and Sarfraz Nawaz Brohi. "E-Government Cybersecurity Modeling in the Context of Software-Defined Networks." *Cybersecurity Measures for E-Government Frameworks*. IGI Global, 2022. 1-21.

Ujjan, R.M.A., Khan, N.A. and Gaur, L., 2022. E-Government Privacy and Security Challenges in the Context of Internet of Things. In *Cybersecurity Measures for E-Government Frameworks* (pp. 22-42). IGI Global.

Ujjan, R. M. A., Hussain, K., & Brohi, S. N. (2022). The impact of Blockchain technology on advanced security measures for E-Government. In *Cybersecurity Measures for E-Government Frameworks* (pp. 157-174). IGI Global.

Ujjan, R. M. A., Taj, I., & Brohi, S. N. (2022). E-Government Cybersecurity Modeling in the Context of Software-Defined Networks. In *Cybersecurity Measures for E-Government Frameworks* (pp. 1-21). IGI Global.

V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, “Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, vol. PP, no. c, p. 1, 2021.

Y. Zhi, Z. Fu, X. Sun, and J. Yu, “Security and Privacy Issues of UAV: A Survey,” Mobile Networks and Applications, vol. 25, no. 1, pp. 95–101, 2020.

Y. M. Kwon, J. Yu, B. M. Cho, Y. Eun, and K. J. Park, “Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles,” IEEE Access, vol. 6, pp. 43 203–43 212, 2018.

Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, “Efficient drone hijacking detection using two-step GA-XGBoost,” Journal of Systems Architecture, vol. 103, pp. 1414–1419, 2020.

Z. Li, C. Gao, Q. Yue, and X. Fu, “Toward Drone Privacy via Regulating Altitude and Payload,” 2019 International Conference on Computing, Networking and Communications, pp. 562–566, 2019.