Chapter 17
Privacy-Preserving Techniques for Drone Surveillance Data: Challenges, Solutions, and Future Directions

Saroj Kushwah
https://orcid.org/0000-0001-7362-9991
Ajay Kumar Garg Engineering College, Ghaziabad, India

Updesh Kumar Jaiswal
https://orcid.org/0009-0002-1572-8275
Ajay Kumar Garg Engineering College, Ghaziabad, India

Jaishree Jain
https://orcid.org/0000-0003-0173-7664
Ajay Kumar Garg Engineering College, Ghaziabad, India

Sadiq Abubakar Maidugu
Sharda University, Greater Noida, India

Bharat Singh
Sanskriti University, Mathura, India

Shashank Sahu
https://orcid.org/0000-0001-6720-4284
Ajay Kumar Garg Engineering College, Ghaziabad, India

Khushbu Malviya
Ajay Kumar Garg Engineering College, Ghaziabad, India

Sandeep Yadav
Ajay Kumar Garg Engineering College, Ghaziabad, India

ABSTRACT

Drone technology has come a long way in the past few years. It is now a vital aspect of smart city development, traffic monitoring, and farming. But using drones to collect and broadcast real-time aerial data on a large scale raises serious privacy concerns. This chapter talks about the main privacy issues with drone surveillance systems, focusing on how they collect, send, store, and analyse data. This chapter also talks about significant areas of research for the future, such as designing cryptographic algorithms that are light, AI-powered privacy controls, privacy rules that are aware of the context, and real-time privacy adaptation. There is a lot of talk about how crucial it is for technologists, lawyers, and policymakers to work together to develop complete privacy standards for drone monitoring. This chapter is aimed to aid

DOI: 10.4018/979-8-3373-4277-1.ch017

anyone who works in academia, engineering, or making decisions who wishes to build drone systems that are safe and don't invade people's privacy. It balance between people's rights and new technology when aerial data surveillance is becoming more common.

1. INTRODUCTION

After initially being primarily linked to military operations, drones have developed into essential tools in fields including construction, agriculture, disaster relief, and surveillance (Cordill et al., 2025). The ability to easily guide the drones to the required locations for video capturing and streaming is one of the essential services. Drones transmit these videos wirelessly to the control centre, where they are saved on cloud servers for later examination. For the purpose of carrying out their particular services, different clients may have access to this video data. The recorded recordings may, however, contain sensitive information about persons that should not be made public, as one might anticipate. According to (Rabieh et al., 2020) people are reluctant to divulge personal information that could be used for identification and tracking, such as their current position (Yahuja, 2021).

Numerous cities worldwide are experiencing population expansion. In light of this, 4.2 billion people live in cities worldwide as of 2018, up from 751 million in 1950, according to UN figures. In addition, the UN predicts that by the middle of the century, there will be a 68% increase in the population of cities and by 2030, there will be 43 megacities with a population of at least 10 million. In this sense, the relatively new idea of the "smart city" can help city administration officials address the problems associated with urbanisation and expansion in a more sustainable and effective manner. Smart cities are large, complex systems (or frameworks) that use a range of various technologies, mostly those based on the Internet of Indicators of smart cities include smart government, economy, the environment, people, living conditions, and mobility. However, it is crucial to remember that good smart city plans would depend less on technology solutions and more on the discovery and implementation of a reasonable approach that could fulfil the requirements, aspirations, and values of all municipal actors and people (Feng et al., 2021).

This chapter goes into detail on the privacy issues that come up when drones collect data. It gives a structured look at the problems that now exist, looks into the best remedies available, rates how well they work, and suggests potential paths for the future. This chapter's goal is to help stakeholders design drone surveillance systems that are both new and respectful of privacy by giving them a multi-dimensional view that includes technological, legal, and ethical factors.

In Privacy Preserving Machine Learning (PPML), Differential Privacy (DP) is a potent technique that ensures statistical preservation of individual privacy. It accomplishes this by carefully introducing noise into the data, making it impossible for an attacker—even one with some prior knowledge—to learn important information about any specific person by looking at the answers to queries or analysis, offers a privacy guarantee that is rigorously suitable for a range of machine learning problems, including regression and classification. This permits customization according to demands and provides trade-offs between privacy and usefulness. Adding noise can make results less accurate. It can be difficult to strike the ideal privacy-utility balance. It might not work with every kind of data or query.

Therefore, we take into consideration drones that have wireless communication capabilities. They have at least one WiFi module, either built within the device or linked as an external accessory, that operates in the 2.4 GHz band (and maybe the 5 GHz band). Usually within a certain range from the drone's