I. I NTRODUCTION

The drone surveillance system is made to watch or find designated objects. This objective is a suitable scenario for the implementation of deep learning, yet the efficiency of its security must be maintained. Unexpected events i.e., natural disaster may occur that needs advance technological equipment. Conventional drone cameras are well-designed torecognize a common human face with or without artificial intelligence processing, but in this research, another case of the drone surveillance system is designed and implemented which will recognize specific customized objects at once [1], [2]. To handle the security measures, improvements on the encryption were also implemented rather than using conventional cryptography system to face the quantum era and to test the efficiency of post-quantum cryptography scheme along with reducing computation power of the device.

Computer vision is extensively used in object detection in critical locations, campuses, industry, and government. Computer vision technology is one of the encouraging scopes of research in drones within the area of computer science, especially deep learning. Machine learning and deep learning have altered computer vision technology. Many deep learning techniques in drones have been proposed recently e.g., improving the YOLOv2 for video-based real-time drone detection [3], a lightweight version of the YOLOv3 architecture [4], outstanding results from YOLOv2 and SSD-Caffe on Jetson TX1, TX2, and AGX Xavier [5]. Over the years, the usage of internet of things hardware keeps increasing. It leads to better improvement on the processing power of the internet of things devices. To provide base benchmark results for the internet of things devices, a common internet of things device of Raspberry Pi 4 (RPi-4) was used without an additional computation module [6], [7]. With only a CPU processing power, the benchmark could be used as a benchmark point of internet of things devices utilization in other related surveillance scenarios. Thus, this research uses the custom configuration in RPi-4 with PiCamera attached in drone DJI Phantom 3, and juxtaposes with YOLOv2, YOLOv3, and YOLOv4. The contributions of this research are as follows:

1. Providing benchmark data of the internet of things devices with NTRU encryption for streaming scenarios.
2. Proposing a wireless streaming protocol with deep learning and post-quantum cryptography implementation.
3. Comparing the usage of NTRU security levels with various deep learning algorithms.
4. Presenting analysis to gain the optimal configuration of CPU only for a drone surveillance system with deep learning and post-quantum cryptography.

The Section II reviews existing works in deep learning-based object detection while Section III explains the proposed approach to securing connection during drone movement. Then, specific aspects of the latest deep learning version (i.e., YOLOv4) and post-quantum cryptography (i.e., NTRU encryption) experiments are described in Section IV. Finally, Section V gives the conclusions and future recommendations of this research.