­

 

Title

By

Name

to

The School of Computing

for the BSc in Computer Science

Thesis Supervisor

Plageras Andreas

Module Professor

Tasos Stylianou

University of Derby

Mediterranean College

2022

**Acknowledgements**

I would first like to thank…

**Abstract** |

KEYWORDS |

**Table of Content**

[1. Introduction 4](#_Toc72153352)

[1.1 Current Study Overview 4](#_Toc72153353)

[1.2 Scientific Contribution 4](#_Toc72153354)

[1.3 Overview 4](#_Toc72153355)

[2. Related Work 6](#_Toc72153356)

[2.1 General 6](#_Toc72153357)

[2.2. Topic analysis of referenced literature 6](#_Toc72153358)

[3. Proposed Work 9](#_Toc72153359)

[3.1. Scientific Context 9](#_Toc72153360)

[3.1.1 Machine Learning in General 9](#_Toc72153361)

[3.1.2 Autonomous Vehicles 10](#_Toc72153362)

[3.2. Sensor System 12](#_Toc72153363)

[3.2.1 Introduction to LiDAR sensor system 12](#_Toc72153364)

[3.2.2 Sensors 12](#_Toc72153365)

[3.3. Proposed Idea 15](#_Toc72153366)

[3.3.1 Idea on Object Recognition 15](#_Toc72153367)

[3.3.2 Need for Improvement 15](#_Toc72153368)

[3.3.3 Upgraded Object Recognition 16](#_Toc72153369)

[3.3.4 Machine Learning Algorithms 20](#_Toc72153370)

[3.4. Idea Implementation 22](#_Toc72153371)

[3.4.1 Project Idea 22](#_Toc72153372)

[3.4.2 Important Software 23](#_Toc72153373)

[3.4.2 Methodology 24](#_Toc72153374)

[4. Comparative Analysis and Discussion 26](#_Toc72153375)

[4.1 Discussion and Challenges 26](#_Toc72153376)

[4.2. Results 26](#_Toc72153377)

[6. Conclusion 27](#_Toc72153378)

[7. Bibliography 29](#_Toc72153379)

**List of figures**

|  |  |
| --- | --- |
| **Figure Number** | **Page** |
| **(1)** | **11** |
| **(2)** | **13** |
| **(3)** | **25** |
| **(4)** | **25** |

**List of tables**

|  |  |
| --- | --- |
| **Table Number** | **Page** |
| **(1)** | **14** |
| **(2)** | **20** |

**List of Abbreviations**

|  |  |
| --- | --- |
| **Abbreviation** | **Text** |
| BD | Big Data |
| CC | Cloud Computing |
| IoT | Internet of Things |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Introduction

Εδώ θα μπεί πρώτα το κομμάτι 2 του Ethical Form…

Έπειτα θα πρέπει αφού εισάγουμε τον αναγνώστη στο θέμα και τη σημαντικότητα της εργασίας να αναφέρουμε τον σκοπό και τους στόχους της εργασίας (κομμάτι 1 του Ethical Form)…

## Current Study Overview

## Scientific Contribution

## 1.3 Outline

Εδώ θα μπεί το κομμάτι 3 του Ethical Form….

Αυτά αρχικά για να αρχίσουμε να δομούμε παράλληλα και το Introduction section το οποίο θα ολοκληρώσουμε στο τέλος…

# 2. Related Work

The internet of things is a very sophisticated network of devices that are capable to connect with each other and provide a very useful service. These devices, can either gather useful information via sensors, interact with the world through various actuators or do both. Throughout the years Drones evolved significantly and became an essential part of the fascinating internet of things and have provided a wide range of services through various applications. It is no secret that drones will control the low aerial space in years to come. With the increasing number of drones into the low aerial space traffic management has become challenging, also due to very sensitive data transfer via drones security concerns have raised that need to be accessed.

Labib, N.S., Brust, M.R., Danoy, G. and Bouvry, P. (2021). The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles. *IEEE Access*, 9, pp.115466–115487.

The Internet of drones (IoD) is the layered network architecture that drones utilize to coordinate navigate to the lower aerial space. It is conducted into layers:

Lin, C., He, D., Kumar, N., Choo, K.-K.R., Vinel, A. and Huang, X. (2018). Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Communications Magazine*, 56(1), pp.64–69.

In recent years, UAV applications for civil and military purposes have been increased significantly. This is because drones are very cost efficient to maintain and can provide very useful information with a bird-eye-view and deliver packages in hard-to-reach locations. Some fields that drones are used are courier services, search and rescue operations, security surveillance etc. Artificial intelligence and more specifically machine learning has a very solid contribution into the development of more complex and utilitarian applications. Therefore, this broad range of applications have caused security threats that need to be managed. Drones handle very sensitive data with a form of audio video or image through communication channels such as WIFI which is not the most secure protocol for data transfer. The biggest security concerns are spoofing, false data injection, jamming etc. The most common way to counterattack these threats is via data encryption during transform.

Shafique, A., Mehmood, A. and Elhadef, M. (2021). Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access*, 9, pp.46927–46948.

The number of drones that are been used for a variety of applications is increasing rapidly day by day. The latter has raised security safety, and privacy concerns. Drones are not always designed with safety in mind and that can lead to unpleasant events such as physical accidents for example (Drones falling and injuring civilians). Furthermore, research have shown that drones can be vulnerable to spoofing, malware infection, data interference and injection, Wi-Fi jamming etc. Additionally, a big issue is the possibility of violation of personal space, drones can reach places and record video or take photos of people without their consent. Based on data that was collected by the Canadian Public safety such incidents have caused a lot of trouble and had led to blackmailing and other unpleasant events. The concerns that were mentioned above can be counter-attacked through data encryption, multi-factor authentication protocols, anti-malware software, and strict legislations according to flight protocols for UAVs from governments.

Yaacoub, J.-P. and Salman, O. (2020). Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations. *Internet of Things*, [online] p.100218. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/.

Πρώτο Task για 8/12/2021 ή εως 11/12/2021

Από μία παράγραφο για το κάθε ένα από τα 5 papers πάνω στο θέμα σας, η οποία θα προκύψει από την περίληψη και τα συμπεράσματα του καθενός.

# 3. Comparative Analysis and Discussion

# 4. Proposed Idea…

# 5. Experimental Results (Testing/Evaluation)

Σε αυτό το σημείο θα έχουμε τα αποτελέσματά μας είτε αυτά είναι από υλοποίηση είτε από συγκριτική ανάλυση της ιδέας μας έναντι άλλων παρεμφερών.

# 6. Conclusion

# 7. Future Work and Directions

# 8. Bibliography