|  |  |  |
| --- | --- | --- |
| **Kingdom of Saudi Arabia**  **Ministry of Education**  **Majmaah University**  **Deanship of Graduate Studies**  **College of Computer and Information Sciences**  **Department of (IT)** | http://faculty.mu.edu.sa/public/uploads/image/20120429/20120429001036_30380.jpg | |
| **Detecting intrusions in the Internet of Drones with**  **an IoT-enabled smart cybersecurity framework**  **Project report submitted in partial fulfillment of the requirements for the award of the Degree of MS in Cybersecurity and Digital Forensics (CSDF)**  **By**  **Abdullah Jamal Al-Fuwaiers**  **441104422**  **Under the Esteemed Guidance of**  **Dr. Shailendra Mishra**  **Professor**  **Department of Information Technology**  **2023-2024** | |

Contents

[Acknowledgement 5](#_Toc165813993)

[Certificate 6](#_Toc165813994)

[Abstract 7](#_Toc165813995)

[Lists of table 8](#_Toc165813996)

[Lists of Figures 8](#_Toc165813997)

[Abbreviation 9](#_Toc165813998)

[Chapter 1 10](#_Toc165813999)

[Introduction 10](#_Toc165814000)

[1.1 Introduction: 10](#_Toc165814001)

[1.2 Background 10](#_Toc165814002)

[1.3 Research Challenges 12](#_Toc165814003)

[1.4 Research Aim and Objective: 14](#_Toc165814004)

[Objectives: 14](#_Toc165814005)

[**1.5 Research Motivation** 15](#_Toc165814006)

[1. Increasing Reliance on Drones: 15](#_Toc165814007)

[2. Growing Sophistication of Cyber Threats: 15](#_Toc165814008)

[3. Urgency of Proactive and Adaptive Cybersecurity: 15](#_Toc165814009)

[4. Safeguarding Critical Applications: 15](#_Toc165814010)

[5. Ensuring Public Safety: 16](#_Toc165814011)

[6. Preserving Privacy: 16](#_Toc165814012)

[7. Unlocking the Full Capabilities of Drones: 16](#_Toc165814013)

[8. Mitigating Risks Associated with Malicious Activities: 16](#_Toc165814014)

[1.6 Research Questions 16](#_Toc165814015)

[1.7 Statement of Problems 17](#_Toc165814016)

[1.8 What has been done so far & how this research is better? 17](#_Toc165814017)

[**1.9 Significance of the Study:** 17](#_Toc165814018)

[**1.10 Structure of the thesis:** 18](#_Toc165814019)

[Chapter 2 18](#_Toc165814020)

[Literature Review: 18](#_Toc165814021)

[**2.1 Introduction to Integration of drone and ioT** 19](#_Toc165814022)

[2.2 Related Articles & Cybersecurity Majors: 20](#_Toc165814023)

[2.3 Research Gaps and Challenges: 26](#_Toc165814024)

[2.4 Findings of Literature Review 26](#_Toc165814025)

[2.5 Conclusions 27](#_Toc165814026)

[Chapter 3 28](#_Toc165814027)

[Research methodology 28](#_Toc165814028)

[**3.1 Qualitative, Quantitative or Mixed Method** 28](#_Toc165814029)

[**3.2 Research design** 28](#_Toc165814030)

[**3.3 Choosing of Research Methods** 28](#_Toc165814031)

[**3.4 Machine learning models** 28](#_Toc165814032)

[**1.** **KNN:** 28](#_Toc165814033)

[**2.** **Naïve Bayes:** 28](#_Toc165814034)

[3. Random Forest 28](#_Toc165814035)

[**4.** **Decision tree:** 28](#_Toc165814036)

[5. LSTM 28](#_Toc165814037)

[3.5 Dataset 28](#_Toc165814038)

[**Research Management plan** 28](#_Toc165814039)

[**3.4 conclusions** 28](#_Toc165814040)

[Chapter 4 28](#_Toc165814041)

[Implementation and Results 28](#_Toc165814042)

[**4.1 Introduction** 28](#_Toc165814043)

[**4.2 Details of the Project Implementation:** 28](#_Toc165814044)

[Tools and techniques: 28](#_Toc165814045)

[**4.3 Implementation setup** 28](#_Toc165814046)

[Performance metric Evaluation: 28](#_Toc165814047)

[**4.4 Experiment Analysis** 28](#_Toc165814048)

[Import libraries 28](#_Toc165814049)

[**Exploratory Data Analysis (EDA)** 28](#_Toc165814050)

[Data visualization 28](#_Toc165814051)

[**Data cleaning** 28](#_Toc165814052)

[**Splitting data:** 28](#_Toc165814053)

[**Scaling:** 28](#_Toc165814054)

[**Machine learning Models implementation** 28](#_Toc165814055)

[KNN 28](#_Toc165814056)

[**Naïve Bayes** 28](#_Toc165814057)

[**Random Forest:** 28](#_Toc165814058)

[**Decision tree:** 28](#_Toc165814059)

[**Conclusions** 28](#_Toc165814060)

[Chapter 5 28](#_Toc165814061)

[Results analysis and Discussions 28](#_Toc165814062)

[**5.1 Introduction** 28](#_Toc165814063)

[**5.2 Results Analysis** 28](#_Toc165814064)

[Results Summary and Analysis 28](#_Toc165814065)

[**5.3 Discussions** 28](#_Toc165814066)

[Model Comparison 28](#_Toc165814067)

[**Robust intrusion detection in real world applicability** 28](#_Toc165814068)

[**Implications for cybersecurity strengthening defenses** 28](#_Toc165814069)

[**Comparative Analysis with Previous Research** 28](#_Toc165814070)

[**5.5 Novelty of this Research** 28](#_Toc165814071)

[**5.4 Conclusions** 28](#_Toc165814072)

[Chapter 6 28](#_Toc165814073)

[Conclusion and future work 28](#_Toc165814074)

[**6.1 Introduction** 28](#_Toc165814075)

[**6.2 Conclusion** 28](#_Toc165814076)

[**6.3 Limitation of the study** 28](#_Toc165814077)

[**6.4 Scope of Future Work** 28](#_Toc165814078)

[References 28](#_Toc165814079)

# Acknowledgement

I want to thank my Lord, Allah, for providing me with the knowledge, guidance, and courage to complete this academic adventure. This all became possible by the Grace of Almighty Allah, who granted me the strength and wisdom to navigate this journey. I am deeply indebted to several individuals whose invaluable support and guidance were instrumental in my success.

Firstly, I extend my heartfelt thanks to my parents, whose unwavering support and encouragement have been the foundation of my achievements. To my father, thank you for instilling in me the values of perseverance and discipline, and for always believing in my potential. To my mother, your love, care, and endless sacrifices have been a constant source of strength and comfort. I couldn't have done this without you both.

I also wish to thank my brother for his constant encouragement and for being a source of motivation throughout my studies. Your positive energy and insightful advice have made this journey much easier.

I would like to thank my supervisor, Dr. Shailendra Mishra, for his expert guidance and patience. His insights and feedback have been instrumental in shaping this thesis. I am grateful for his dedication and the time he devoted to helping me refine my work.

Additionally, I acknowledge the invisible hand that has guided me through challenging times, providing me with the strength to keep moving forward. To the unseen forces that brought supportive people into my life, I am forever grateful.

Thank you to all who have been a part of this journey, whether through direct support, inspiration, or simply believing in me. This thesis is a testament to the power of community and the blessings that come from those around us.

Sincerely.

Abdullah Jamal Alfuwaiers

# **Certificate**

This is to certify that the project report entitled " Detecting intrusions in the Internet of Drones with an IoT-enabled smart cybersecurity framework" being submitted by Abdullah Jamal A. Alfuwaiers (ID 441104422) in partial fulfillment for the award of Degree of MS in Cybersecurity and Digital Forensics (MSCSDF) to the Department of IT, College of Computer Sciences, Majmaah University is a record of authentic work carried out under my guidance and supervision. the results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree or Diploma.

****

**Dr. Shailendra Mishra**

(Supervisor)

Professor

Department of IT

College of Computer & Information Sciences

Majmaah University

Head of the Department

# Abstract

Drones are becoming increasingly important in smart cities, agriculture, surveillance, and other industries; nevertheless, because of their internet connection, they provide weaknesses that might be exploited by bad actors. In order to tackle this issue, we put forth a comprehensive cybersecurity architecture that utilises the intersection of machine learning (ML) algorithms and Internet of Things (IoT) technologies to identify and prevent breaches inside the Internet of Drones (IoD). Our architecture connects a network of IoT-enabled sensors and devices that are placed strategically across the drone ecosystem. This network continuously collects and analyses data on system behaviours, communication patterns, and environmental variables. The collected data is then sent into a centralised platform that has sophisticated machine learning algorithms, including models for pattern identification and anomaly detection. This platform carefully examines the data to find anomalous activity that can indicate possible security risks. Our framework's dynamic learning mechanism, which constantly adjusts to changing threats enabling real-time intrusion detection, is one of its primary features. By combining IoT and ML technologies, the system is able to distinguish between typical and abnormal activity, which creates a proactive defence against cyberattacks on the IoD infrastructure. Moreover, our approach prioritises the protection of data integrity and confidentiality by highlighting the need of safe communications protocols and cryptographic algorithms. We carefully evaluate the effectiveness of our suggested framework in various IoD scenarios using extensive simulations and tests. The outcomes highlight its ability to quickly and reliably identify different kinds of intrusions. This validation procedure informs future improvements and modifications while also demonstrating the framework's effectiveness. This study aims to tackle the cybersecurity issues brought about by the incorporation of drones into many industries. Our suggested architecture aims to strengthen the IoD ecosystem by securing a safe and robust context for drone-enabled applications in our networked world, bolstered by the symbiosis of IoT and ML technologies.

# **Lists of table**

[Table 1 Summary or literature reviews 19](#_Toc165813448)

[Table 2summarizing the results for each algorithms 66](#_Toc165813449)

[Table 3 Comparative Analysis with Previous Research 70](#_Toc165813450)

# **Lists of Figures**

[Figure 1architecture for industrial drones. 11](#_Toc165813296)

[Figure 2 research framework 30](#_Toc165813297)

[Figure 3 KNN working 35](#_Toc165813298)

[Figure 4 k factor 36](#_Toc165813299)

[Figure 5 Naive Bayes 37](#_Toc165813300)

[Figure 6 Random forest 38](#_Toc165813301)

[Figure 7 equation of random forest 39](#_Toc165813302)

[Figure 8 calculate entropy 39](#_Toc165813303)

[Figure 9 Decision tree 40](#_Toc165813304)

[Figure 10 LSTM 41](#_Toc165813305)

[Figure 11 NSLKDD dataset 41](#_Toc165813306)

[Figure 12 performance measure formula 47](#_Toc165813307)

[Figure 13 import libraries 48](#_Toc165813308)

[Figure 14 missing values 49](#_Toc165813309)

[Figure 15 Data info 49](#_Toc165813310)

[Figure 16 Data visualization 51](#_Toc165813311)

[Figure 17 most service used 52](#_Toc165813312)

[Figure 18 http service used 53](#_Toc165813313)

[Figure 19 imbalance dataset 54](#_Toc165813314)

[Figure 20Correlation matrix 55](#_Toc165813315)

[Figure 21 data cleaning 56](#_Toc165813316)

[Figure 22 missing data 57](#_Toc165813317)

[Figure 23 encoding data after numerical 58](#_Toc165813318)

[Figure 24 outliers as box plot 59](#_Toc165813319)

[Figure 25 removed outliers from dataset 60](#_Toc165813320)

[Figure 26Confusion matrix of KNN 61](#_Toc165813321)

[Figure 27 confusion matrix for naive bayes 62](#_Toc165813322)

[Figure 28 confusion matrix for random forest 63](#_Toc165813323)

[Figure 29 Confusion matrix for Decisiontree 64](#_Toc165813324)

[Figure 30 model comparison 69](#_Toc165813325)

[Figure 31 precision recall and f1 score 70](#_Toc165813326)

# **Abbreviation**

|  |
| --- |
| IoT Internet of Things |
| IDS Intrusion Detection System |
| ML Machine Learning |
| KNN K-Nearest Neighbors |
| NSL-KDD Network Security Laboratory KDD |
| UAV Unmanned Aerial Vehicle |
| EDA Exploratory Data Analysis |
| RMSE Root Mean Squared Error |
| MAE Mean Absolute Error |
| R^2 Coefficient of Determination |
| API Application Programming Interface |
| LSTM Long Short-Term Memory |
| DNS Domain Name System |
| HTTP Hypertext Transfer Protocol |
| UDP User Datagram Protocol |

# Chapter 1

# Introduction

The integration of internet of things iot technologies with unmanned aerial vehicles commonly known as drones has ushered in a new era of possibilities and challenges as drones become increasingly prevalent across various industries ranging from agriculture and surveillance to emergency response their reliance on iot enabled communication introduces a complex web of security considerations this chapter serves as a gateway to understanding the intricate landscape of securing the internet of drones iod within a cybersecurity framework.

# 1.1 Introduction:

The internet of things io t is a rapidly evolving field of technology that has impacted almost every aspect of our lives including drones or drones the integration of drones into the io t paradigm opens up unprecedented opportunities for applications ranging from surveillance to delivery services however this expansion also introduces novel challenges particularly in the critical domain of cybersecurity this research aims to tackle the pressing issue of detecting intrusions in the internet of drones by introducing and implementing an innovative io t enabled smart cybersecurity framework [1].

## 1.2 Background

The convergence of internet of things io t and drone technologies holds immense promise ushering in a new era of possibilities this amalgamation however is not without its challenges particularly in the realm of cybersecurity the vulnerabilities inherent in this integration necessitate a comprehensive and forward thinking approach to secure the communication channels and ensure the data integrity of interconnected drones traditional security measures designed for more conventional networks may fall short in addressing the intricacies of this dynamic and distributed system [2].

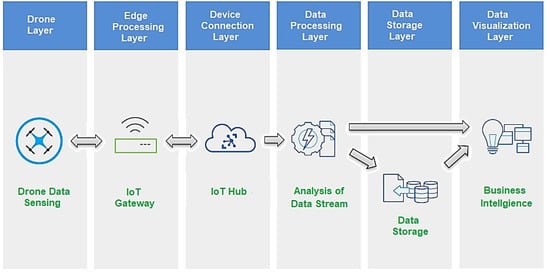


Figure 1architecture for industrial drones.

Drones are rapidly evolving from standalone devices to integral components within io t ecosystems this paradigm shift brings forth a pressing need for an advanced cybersecurity framework that strategically leverages the unique capabilities of io t technologies as drones become increasingly integrated into various sectors from agriculture and surveillance to logistics and emergency response the stakes for securing these systems have never been higher the dynamic nature of drone communication is a defining characteristic marked by rapid data exchange and unprecedented mobility unlike static devices in traditional networks drones operate in diverse and distributed environments presenting a plethora of security challenges the fluidity and complexity included in io t enabled drones may be difficult for conventional security methods to adjust to as they were created with more predictable network topologies in mind as such tackling these issues calls for an advanced context aware cybersecurity strategy that is especially designed for the complexities of the internet of drones drones need for real time communication is one of the main obstacles these gadgets often transmit data quickly and continuously to carry out operations including cooperative missions real time monitoring and navigation many security methods are rigid and old which might impede smooth information flow between drones and result in communication process vulnerabilities or slowness furthermore another level of intricacy is added by the drones mobility drones may operate in a variety of uncertain conditions such as isolated locations agricultural fields and urban landscapes and they can cover large geographic regions in this dynamic operating context where drones fly between several communication nodes and meet a variety of network circumstances traditional security solutions find it difficult to adjust this motion presents difficulties in maintaining the wide variety of uses for internet of things enabled drones also adds another piece to the security problem every application has different security needs whether it is used for package delivery search and rescue operations surveillance or precision agriculture in order to meet the unique requirements of every application inside the internet of drones a customised and adaptable architecture is necessary rather than a one size fits all approach to cybersecurity a smart and context aware cybersecurity solution is essential to meet these problems the distinct qualities of io t enabled drones such as their many uses mobility and dynamic communication patterns should be taken into account in this strategy it is critical to implement security protocols that can encrypt sensitive data during transmission authenticate devices in real time and dynamically adapt to changing situations machine learning algorithms have the potential to improve the adaptability of cybersecurity frameworks for drones that are connected to the internet machine learning algorithms may identify abnormalities and possible intrusions in real time by continually examining patterns of behaviour and communication this proactive defence against ever evolving threats is made possible moreover the application of blockchain technology offers a novel way to improve the transparency and integrity of data transfers between drones equipped with internet of things capabilities the information sent between drones is secure and unmodified because to blockchain s decentralised and tamper resistant design which allays worries about data integrity in dynamic and scattered contexts [3].

## 1.3 Research Challenges

In navigating the intricate terrain of integrating the internet of things io t with drone technology a multitude of challenges emerges surpassing the bounds of traditional cybersecurity concerns the decentralized nature of drone networks sprawling across vast expanses poses a formidable challenge to conventional security measures designed for more centralized systems adapting to this distributed architecture requires the development of security protocols that exhibit adaptability and scalability ensuring consistent protection across various nodes without relying on a centralized authority compounding this challenge is the inherent resource constraints of unmanned vehicles drones crafted for agility and lightness grapple with limited processing power memory and energy resources achieving a delicate equilibrium between implementing robust security measures and preserving operational efficiency necessitates the development of resource efficient security protocols this involves the optimization of encryption algorithms authentication processes and intrusion detection mechanisms to operate seamlessly within the confines of the drone s limited resources [4].

Adding to the complexity is the dynamic communication patterns intrinsic to drones their rapid and adaptive communication characterized by altering routes and engaging with diverse network conditions necessitates security measures capable of seamless adjustment tackling this challenge entails the development of communication protocols and encryption methods that can dynamically adapt to changing conditions this ensures continuous protection of data exchanges without impeding the flexibility required for the drone s operational effectiveness a profound understanding of the specific vulnerabilities and threats associated with both io t and drone technologies stands as a foundational challenge researchers and practitioners are compelled to delve into the intricacies of drone operations communication protocols and the unique security challenges introduced by io t integration bridging knowledge gaps through interdisciplinary collaboration between experts in drone technology communication systems and cybersecurity is imperative to devise holistic security strategies [5].

Sophisticated intrusion detection mechanisms tailored to the nuances of io t enabled drones present another formidable challenge traditional intrusion detection systems calibrated for static networks may falter in identifying and responding to intrusions in the dynamic and dispersed environment of io t enabled drones addressing this challenge involves the exploration of machine learning algorithms capable of adapting to the evolving threat landscape learning from historical data to identify anomalies and potential security threats in real time identifying subtle deviations from normal patterns of operation indicative of potential security threats presents yet another layer of complexity advanced anomaly detection techniques including behavior analysis and statistical modeling become crucial integrating these techniques into the cybersecurity framework enhances the ability to detect abnormal behavior in the network providing a proactive defense mechanism against emerging cyber threats seamlessly integrating advanced technologies such as machine learning and blockchain into the cybersecurity framework without causing operational disruptions emerges as a pivotal challenge leveraging the full potential of these technologies requires meticulous consideration of their implementation within the existing architecture this involves the development of protocols and mechanisms that can integrate with the diverse components of io t enabled drone systems while maintaining a high level of security the adaptability of security measures to the evolving threat landscape is a perpetual challenge the dynamic nature of cyber threats necessitates continuous monitoring regular updates and a proactive stance towards emerging challenges this challenge involves developing security frameworks capable of evolving alongside the threat landscape anticipating potential risks and adapting defenses accordingly tailoring security measures to the specific needs of applications whether in precision agriculture surveillance or package delivery underscores the challenge of accommodating diverse requirements this necessitates a nuanced understanding of the unique security challenges posed by each use case [6].

## 1.4 Research Aim and Objective:

The main goal of this effort is to provide a customised and flexible cybersecurity architecture for the internet of drones taking into account the particular difficulties posed by data manipulation communication eavesdropping and unauthorised access by doing this the study hopes to create a strong security framework that guarantees the availability confidentiality and integrity of data in drone systems that are enabled by the internet of things.

### Objectives:

* Use algorithms based on machine learning to find trends in IoT-enabled drone systems' weaknesses and possible threats.
* Use machine learning techniques to determine where improvements may be made and evaluate how well the current security procedures handle security issues unique to drones.
* Integrate machine learning algorithms for adaptive intrusion detection, anomaly detection, and behavior analysis within the cybersecurity framework
* Apply machine learning models to IoT-enabled drone systems to provide real-time threat detection, learning from past data, and continuous monitoring.
* To identify and stop unwanted access, use anomaly detection and authentication methods based on machine learning.

## **1.5 Research Motivation**

This imperative arises at the intersection of technological advancements and potential vulnerabilities inherent in unmanned systems compelling researchers and practitioners to delve into multifaceted motivations the overarching goal is to harness the full capabilities of drones while mitigating the risks posed by malicious activities.

### 1. Increasing Reliance on Drones:

The escalating reliance on drones underscores their transformative impact on industries as these unmanned systems become integral to critical applications their security becomes paramount to ensure the continuity and efficiency of these sectors.

### 2. Growing Sophistication of Cyber Threats:

The increasing sophistication of cyber threats poses a significant risk to the security of io t enabled drones addressing this challenge is essential to protect against potential attacks that could compromise data integrity disrupt operations or even compromise the physical safety of individuals.

### 3. Urgency of Proactive and Adaptive Cybersecurity:

The urgency lies in the need for a cybersecurity framework that anticipates and responds to emerging threats in real time a proactive approach is essential to stay ahead of potential vulnerabilities and ensure the resilience of io t enabled drone systems.

### 4. Safeguarding Critical Applications:

The security of io t enabled drones directly correlates with the reliability and success of critical applications safeguarding these applications ensures the effectiveness of drones in scenarios where human intervention may be limited or impractical.

### 5. Ensuring Public Safety:

Ensuring the cybersecurity of drones is imperative for public safety a breach in drone security could lead to accidents unauthorized access to sensitive locations or even the potential use of drones as weapons developing robust security measures mitigates these risks and fosters safe integration into public spaces.

### 6. Preserving Privacy:

Preserving privacy is a crucial ethical and legal consideration in the deployment of drones a proactive cybersecurity approach safeguards against unauthorized data access and ensures that drones operate within ethical boundaries addressing concerns about unwarranted surveillance or data misuse.

### 7. Unlocking the Full Capabilities of Drones:

By developing a robust cybersecurity framework the research aims to remove barriers that may limit the adoption and deployment of drones this motivation stems from the belief that addressing security challenges will unlock the full capabilities of drones fostering innovation and advancement in diverse sectors.

### 8. Mitigating Risks Associated with Malicious Activities:

The research is driven by the imperative to identify understand and mitigate the risks associated with malicious activities by doing so the aim is to create a secure environment where drones can operate without becoming vectors for cyber threats or physical harm in essence the motivation behind this research recognizes the pivotal role drones play in modern applications and the imperative to secure them against an evolving threat landscape by systematically addressing these challenges the research seeks to contribute to the development of a robust and adaptive cybersecurity framework for the internet of drones ensuring the responsible and secure integration of these unmanned systems into our daily lives.

## 1.6 Research Questions

1. What are the most effective techniques for detecting and preventing intrusions in the Internet of Drones?
2. How does the proposed framework compare to existing cybersecurity solutions for drones?
3. what are the key vulnerabilities in the current io t enabled drone systems
4. how can a smart cybersecurity framework enhance the security of drones in the iot?

## 1.7 Statement of Problems

The integration of drones into the IoT introduces security concerns such as unauthorized access, data tampering, and communication interception. Current cybersecurity measures may not adequately address these issues, necessitating the development of a specialized framework tailored to the unique challenges posed by the Internet of Drones.

## 1.8 What has been done so far & how this research is better?

Previous research in the domain has predominantly focused on conventional security measures for drones within IoT environments, encompassing encryption, authentication, and intrusion detection systems. However, these studies often fall short in addressing the intricate challenges presented by the decentralized structure of drone networks, resource limitations, and dynamic communication patterns. While some efforts have explored the integration of machine learning for anomaly detection, this research significantly advances the field by exclusively emphasizing a specialized and adaptive cybersecurity framework tailored explicitly for the integration of drones into the IoT. This novel approach aims to comprehensively address unauthorized access, data tampering, and communication interception, leveraging machine learning for adaptive intrusion detection and behavioral analysis. By focusing solely on machine learning without incorporating blockchain, the research streamlines its approach, contributing a dynamic and responsive security solution that is more attuned to the unique demands of IoT-enabled drones compared to existing studies.

## **1.9 Significance of the Study:**

This research contributes to the advancement of drone cybersecurity by proposing an innovative framework that integrates IoT and ML technologies. The findings are expected to inform the development of effective, adaptive solutions for securing drones within the broader IoT ecosystem.

## **1.10 Structure of the thesis:**

The remainder of this thesis is organized as follows:

chapter 2 provides a comprehensive literature review highlighting existing research on iot security drone technologies and the intersection of the two

chapter 3 delves into the methodology employed for the research

chapter 4 implement the approach taken in data collection analysis and framework development

chapters 5 present the result findings and discussions

chapter 6 highlight the conclusions drawn from the study offering valuable insights into the intricate realm of securing io t enabled drones against cyber threats.

# **Chapter 2**

# **Literature Review:**

The synthesis of knowledge in the field of internet of things io t security and unmanned aerial vehicles sets the stage for comprehending the intricacies of securing the internet of drones io d this literature review explores existing research frameworks and methodologies related to io t security drone technologies and the converging landscape where these two domains intersect

## **2.1 Introduction to Integration of drone and ioT**

The integration of drones into the Internet of Things (IoT) has prompted a surge of research addressing the complex interplay between unmanned aerial vehicles and cybersecurity. Existing studies have shed light on the conventional security measures employed in IoT-enabled drone systems, emphasizing encryption, authentication, and intrusion detection systems. However, these efforts often fall short in accommodating the decentralized architecture of drone networks and the dynamic nature of their communication patterns. Some notable contributions have explored the application of machine learning techniques for anomaly detection in drone networks. While machine learning shows promise in enhancing security, a critical gap remains in the literature concerning the development of a specialized cybersecurity framework exclusively tailored for the Internet of Drones. This research aims to address this gap by proposing a novel framework that leverages machine learning for adaptive intrusion detection and behavioral analysis, providing a more dynamic and responsive approach to securing IoT-enabled drone systems. By emphasizing a comprehensive and specialized approach, this research seeks to advance the current state of knowledge in IoT security for unmanned aerial vehicles [7].

The prevalence of supervised, unsupervised, and semi-supervised learning in addressing cyber threats, citing examples in communication networks, IoT networks, and cloud computing. [8] highlights the limited research on ML applications in drone network security, introducing an access control mechanism as a novel contribution in the context of drone cybersecurity, distinguishing itself from previous works such as [9] blockchain-based solution that lacked suitability for IoT-based drone networks. The authors [10] devised a novel two-stage model, integrating LSTM and Random Forest, for efficient attack flow detection in network traffic, introduced an LSTM Autoencoder for precise identification of individual attacks with minimal features, analyzed an SVM model for short-duration attack flow detection, and openly shared a low-rate attack dataset on GitHub.

## 2.2 Related Articles & Cybersecurity Majors:

Table 1 Summary or literature reviews

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cite Key | Security Threat & Attacks | Detection & Mitigation | Incident Response | Standards & Policy | Important Findings |
| [11] | ✗ | ✓ | ✓ | ✗ | emphasizes the importance of a security-empowered drone network to prevent interception and intrusion, utilizing a hybrid ML technique that demonstrates enhanced performance in terms of temporal efficacy and statistical measures. |
| [12] | ✓ | ✓ | ✓ | ✗ | proposes a system using deep learning and machine learning techniques for effective detection, with promising evaluation metrics. |
| [13] | ✓ | ✓ | ✓ | ✓ | emphasizes challenges in IoT cybersecurity for government use, highlighting the urgent need for research, policy development, and systematic approaches to address security concerns |
| [14] | ✓ | ✓ | ✓ | ✗ | explores the impact of architectural issues on the security of drone networks, emphasizing the need for a secure Internet of Drones (IoD) to prevent privacy and security threats. |
| [15] | ✓ | ✓ | ✗ | ✗ | Integration of IoT in healthcare systems enhances services but exposes vulnerabilities in data transmission, necessitating security measures. |
| [16] | ✓ | ✓ | ✗ | ✗ | proposed framework utilizes metaheuristic techniques, specifically binary gravitational search algorithm and binary grey wolf optimization, for intelligent cyber threat detection. |
| [17] | ✓ | ✓ | ✓ | ✗ | focuses on the security of cyber–physical satellite systems and IoT-aided aerial vehicle systems, addressing security threats, and proposing an intelligent framework for detection and mitigation |
| [18] | ✓ | ✗ | ✗ | ✗ | highlights the increasing attention towards Unmanned Aerial Vehicles (UAVs) due to their efficiency, cost-effectiveness, and ad hoc network formation capabilities. It specifically focuses on IoT-enabled UAVs and their applications in 3D aerial networks for information processing, communication, and location-based services. |
| [19] | ✓ | ✗ | ✗ | ✗ | Logistic regression is proposed as an approach to estimate statistical possibility in the context of security attacks in IoT-based UAV networks. |
| [20] | ✗ | ✗ | ✗ | ✗ | The classification process utilizes a Deep Belief Network (DBN) combined with a Sparrow Search Optimization (SSO) algorithm. |

## 2.3 Research Gaps and Challenges:

Detecting intrusions in the Internet of Drones (IoD) is a complex challenge that demands a sophisticated cybersecurity framework, particularly in the context of the rapidly evolving threat landscape and the interconnected nature of drones within the IoT ecosystem. While iot technologies provide a wealth of sensor data from drones the current state of cybersecurity lacks a holistic solution that seamlessly integrates this data with machine learning ml algorithms specifically designed for drone security the research focus should emphasize the development of a dynamic defense mechanism that not only enhances detection accuracy but also enables proactive responses to emerging threats ultimately ensuring the integrity and security of internet connected drones this integration of io t and ml technologies represents a pivotal step towards a comprehensive cybersecurity solution for the io d addressing the current gap and providing a foundation for future advancements in drone security.

2.4 Findings of Literature Review

The literature underscores the pivotal role of integrating io t and ml technologies in fortifying drone security with an emphasis on harnessing io t enabled sensors to collect real time drone data researchers advocate for the application of ml algorithms to analyze this data particularly in the realm of intrusion detection existing works highlight the constraints of conventional drone security measures stressing the imperative for advanced adaptive solutions that grapple with challenges such as scalability real time threat detection and the dynamic nature of the internet of drones io d anomaly detection using ml emerges as a focal point lauding ml s prowess in scrutinizing patterns learning from historical data and pinpointing deviations in drone behavior to enhance intrusion detection accuracy privacy and regulatory concerns take center stage in scholarly discourse with researchers delving into the legal and ethical dimensions of drone security within the io t framework emphasizing responsible and transparent ml algorithm use the literature also delves into the exploration of autonomous response mechanisms propelled by ml recognizing the autonomy of ml algorithms to trigger responsive actions in real time as integral to fortifying drone security frameworks acknowledging the complexity of the subject the literature advocates for interdisciplinary approaches urging collaboration across cybersecurity io t and machine learning domains to effectively address the multifaceted challenges inherent in securing the internet of drones.

## 2.5 Conclusions

In conclusion the examination of literature concerning the amalgamation of io t and machine learning ml in the realm of drone security unveils a compelling trajectory geared towards bolstering the resilience of cybersecurity frameworks within the internet of drones io d scholars consistently highlight the importance of utilizing io t enabled sensors to gather real time drone data coupled with the deployment of ml algorithms for sophisticated intrusion detection the literature accentuates the drawbacks of traditional drone security measures underscoring the urgent necessity for adaptive solutions capable of tackling challenges like scalability real time threat detection and the dynamic nature of the io d environment a central focus is on anomaly detection using ml recognizing ml s capacity to scrutinize patterns and detect deviations in drone behavior thereby enhancing the precision of intrusion detection privacy and regulatory concerns are recognized as pivotal elements instigating conversations on the legal and ethical dimensions of drone security within the io t with a strong emphasis on responsible use of ml algorithms additionally the exploration of autonomous response mechanisms powered by ml signals a shift towards real time proactive defense strategies in drone security frameworks lastly the literature consistently advocates for interdisciplinary approaches stressing the importance of collaboration across cybersecurity io t and ml domains to effectively confront the multifaceted challenges inherent in securing the internet of drones overall the literature indicates a dynamic and evolving landscape where the integration of io t and ml holds vast potential for shaping the future of drone cybersecurity.

# **Chapter 3**

# **Research methodology**

The effectiveness of any research endeavor hinges on the rigor and precision of its methodology this chapter delineates the systematic approach employed to investigate and address the cybersecurity challenges inherent in the integration of the internet of things io t with unmanned aerial vehicles commonly known as drones by providing insight into the research design data collection strategies and analytical methodologies this chapter establishes the framework that underpins the subsequent exploration and analysis within this study.

## **3.1 Qualitative, Quantitative or Mixed Method**

The research methodology for the study employs a mixed methods approach seamlessly combining qualitative and quantitative strategies the qualitative facet involves an extensive literature review to establish a theoretical foundation while the quantitative dimension focuses on empirical data collection through the creation of a simulated io t enabled drone environment and the gathering of historical data for ml algorithm training the integration of iot and ml technologies within this simulated environment forms a crucial step configuring sensors to collect real time drone data and feeding it into ml algorithms for intrusion detection evaluation encompasses performance metrics and cross validation techniques to ensure the effectiveness and generalizability of ml models scalability testing involves gradually increasing the number of simulated drones to assess system performance while ethical considerations emphasize privacy safeguards and transparency in ml algorithms interdisciplinary collaboration with cybersecurity iot and machine learning experts enriches the research and if feasible validation with real world drone data adds practical applicability thorough documentation of the entire process from design to analysis aims to contribute valuable insights to the intersection of drone security io t and machine learning.

## **3.2 Research design**

The research design unmanned aerial vehicle uav framework employs a combination of machine learning ml and deep learning dl approaches for intrusion detection io d within uav networks specifically designed to cater to the network structure where drones establish connections with base and ground stations for transaction management the framework comprises two essential components the base station and the ground station both entrusted with the responsibility of capturing and processing data unlike conventional networks with centralized modules the envisioned drone framework necessitates distinct hybrid modules for the base and ground stations the base station module manages all drone communications validating the drone s module selection distributed modules are utilized for detecting and evaluating the level and nature of attacks each drone is equipped with a module dedicated to monitoring attacks directly while a second module is positioned at the ground base station these modules collaborate to validate attacks and determine which drones warrant notification all drones in the airspace can communicate with the base station a singular station or a network of stations the choice between streaming or batching for drone intrusion detection hinges on the technology utilized batch processing becomes essential when employing map reduce as a significant decision making component requiring development time conversely runtime identification can be achieved through frameworks such as flink storm apache kafka or spark in this research apache kafka is favored for its efficient handling of massive data streams especially in the initial stages the study emulates real time analysis by streaming data to the modules in below figure illustrates the layered architecture of drone attacks within the smart framework the framework primarily consists of two components drones and base stations

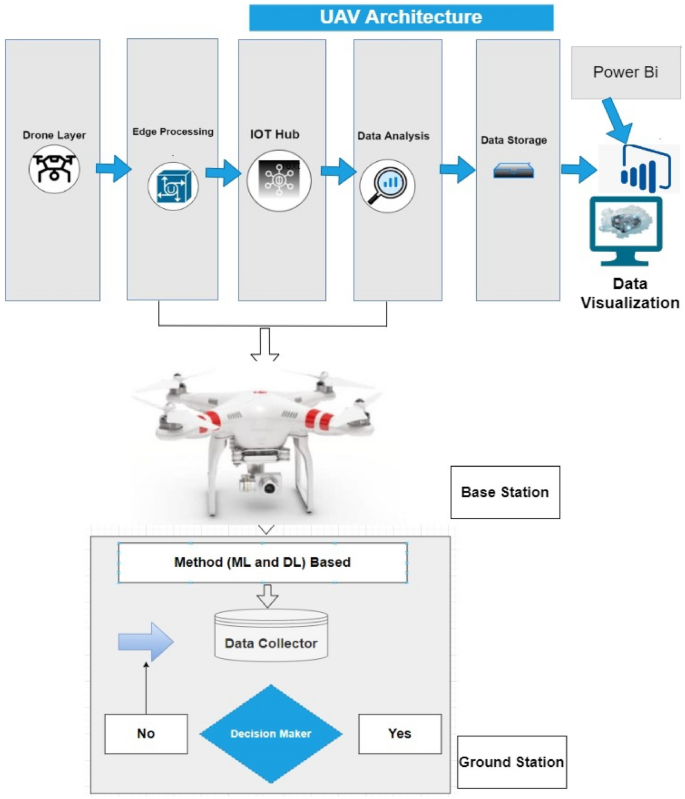


Figure 2 research framework

The proposed model consists of a hierarchical structure with distinct layers for efficient operation in the context of industrial drones at the drone layer camera equipped quadcopters serve as the initial tier collecting io t sensor data through smart sensors like gps radar and altitude sensors an unmanned aircraft system uas drone oversees flight operations and sensor data logging communicating with the ground controller through a specially designed communication link the edge processing layer handles data verification transmission and communication utilizing an azure iot gateway for cloud connectivity this layer plays a crucial role in managing data flow ensuring quick information transfer through wi fi connectivity the subsequent security and privacy layer employs machine learning models for device authentication and access control addressing potential threats to physical behavioral and location privacy authentication procedures combat security concerns like spoofing and intrusion attacks the device connection layer facilitates connectivity through iot gateways ensuring secure connections to the cloud based io t hub for authenticated devices a security orchestration and automation module further enhances device connectivity and real time security through blockchain technology ensuring data integrity and protection on a cloud server this hierarchical structure ensures a comprehensive and secure framework for the internet of drones io d with considerations for data privacy device authentication and secure communication

The integration of IoT sensors, data collection, and machine learning (ML) for s­ubsequent data analysis involves a multi-step process:

1. **IoT Sensor Deployment:**
   * Select and deploy io t sensors on drones or in the drone environment to capture relevant data these sensors could include accelerometers gyroscopes gps modules cameras and other devices capable of collecting various types of data such as movement location and visual information.
2. **Data Transmission to Cloud/Server:**

* Create a communication infrastructure for data transmission from internet of things sensors to a server or centralised cloud this guarantees that the information gathered is centralised and available for additional processing.

1. **Data Preprocessing:**

* Prepare the raw data for analysis by cleaning and organising it beforehand this might entail addressing missing numbers eliminating noise and formatting data so that machine learning algorithms can use it.

1. **ML Algorithm Training:**

* Train machine learning algorithms using the preprocessed data in order to teach the machine learning model to recognise patterns correlations and anomalies linked to both typical and invasive drone behaviour historical data must be fed into it.

1. **Real-time Data Collection:**
   * Make it possible for io t sensors to continually gather data from drones in real time during operating scenarios the continuous flow of data feeds the machine learning model with up to date knowledge so it can adjust and identify emerging trends or abnormalities .
2. **Inference and Anomaly Detection:**
   * Use the trained machine learning model to instantly analyse incoming data based on the patterns discovered during the training stage the machine learning model may identify abnormalities or departures from typical drone behaviour.
3. **Alert Generation:**
   * Create a system that will send out messages or warnings in the event that the machine learning model detects any intrusions or unusual drone activity this guarantees prompt reactions to security risks.
4. **Data Analysis and Visualization:**
   * Perform in depth data analysis on the outcomes produced by the machine learning model this entails assessing intrusion detection accuracy seeing trends in security occurrences and learning more about the security posture as a whole.
5. **Continuous Improvement:**
   * Implement mechanisms for continuous improvement of the ml model this involves periodic retraining with new data to enhance the models accuracy and adaptability to evolving drone behaviors and threats.
6. **Feedback Loop with IoT Sensors:**

* Establish a feedback loop between the ml model and io t sensors insights gained from data analysis can inform adjustments to sensor configurations improving the overall effectiveness of the io t enabled smart cybersecurity framework.

This end-to-end process integrates IoT sensor data collection seamlessly with machine learning for advanced analysis, enabling the development of a dynamic and adaptive cybersecurity solution for the Internet of Drones [21].

## **3.3 Choosing of Research Methods**

In selecting the research methods for this study on iot enabled drone cybersecurity several considerations were taken into account to ensure a comprehensive and effective investigation the chosen methods align with the goals of understanding the intricacies of cybersecurity challenges and proposing a suitable framework the research methods include a combination of exploratory descriptive and analytical approaches.

**Exploratory research:**

The exploratory phase involves an in depth literature review and expert consultations this method is chosen to establish a foundational understanding of iot enabled drone cybersecurity challenges by reviewing existing literature on iot security drone technologies and intrusion detection systems the study aims to identify key concepts variables and potential gaps in current knowledge expert consultations with cybersecurity professionals and drone technologists provide valuable qualitative insights into critical areas of concern and potential research directions.

**Descriptive research:**

Descriptive research is employed to characterize the communication patterns network behaviors and potential threats within the io t enabled drone ecosystem this involves a detailed analysis of the nsl kdd dataset which serves as a representative source of data for understanding common attack patterns and normal behaviors specific to io t enabled drones descriptive methods are crucial in building a comprehensive profile of the cybersecurity landscape within the proposed framework.

**Analytical research**

The analytical phase employs both quantitative and qualitative analysis to derive meaningful insights from the collected data quantitatively statistical tools are applied to identify patterns trends and correlations within the nsl kdd dataset qualitatively content analysis is utilized to extract valuable insights from textual and contextual information this dual approach ensures a nuanced understanding of the cybersecurity challenges faced by io t enabled drones and evaluates the effectiveness of intrusion detection mechanisms.

**limitations consideration:**

The research acknowledges potential limitations associated with the nsl kdd dataset such as its origin in a more generic network intrusion detection context recognizing these limitations is crucial for interpreting the results accurately and understanding the scope of the research the choice of the nsl kdd dataset is made based on its relevance and availability for studying cybersecurity challenges but researchers should remain mindful of its specific context and potential limitations in representing io t enabled drone scenarios in summary the chosen research methods encompass a holistic approach combining literature review expert consultations dataset analysis and simulation to comprehensively address the research objectives these methods are tailored to the unique challenges and complexities of io t enabled drone cybersecurity providing a solid foundation for the subsequent stages of data analysis and framework development.

## **3.4 Machine learning models**

### **KNN:**

K nearest neighbors knn stands as a versatile and intuitive machine learning algorithm employed for both classification and regression tasks operating on the fundamental concept of proximity knn predicts the target variable of a given data point by assessing the majority class or average value among its k nearest neighbors in the feature space the algorithm relies on a distance metric typically euclidean to quantify the similarity between data points although alternative metrics such as manhattan or minkowski can be utilized the decision rule hinges on the majority class for classification tasks.

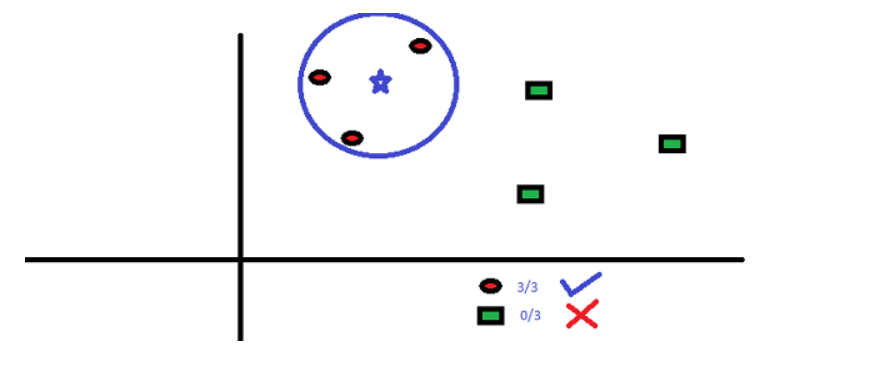
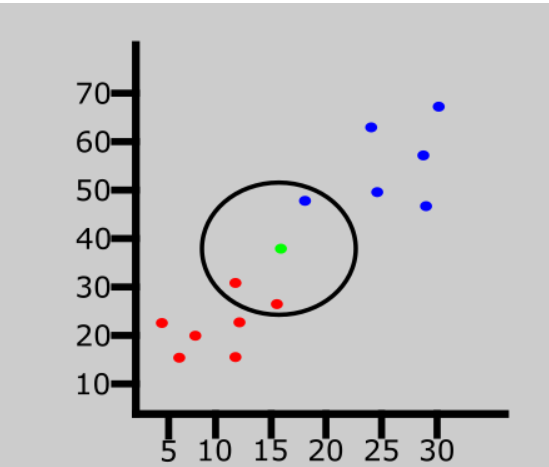


Figure 3 KNN working

While regression tasks involve predicting the average target value of the k nearest neighbors the hyperparameter k representing the number of neighbors considered plays a pivotal role in shaping the model s sensitivity to local patterns by storing the entire training dataset in memory knn bypasses a formal training phase earning its classification as a lazy learner despite its simplicity and ease of implementation.

Figure 4 k factor

Knn exhibits sensitivity to irrelevant or redundant features and can become computationally demanding for large datasets during prediction its applicability is found in various domains such as text classification recommender systems and image data pattern recognition particularly when decision boundaries are non linear and not well defined to optimize knn s performance careful consideration of preprocessing steps including feature scaling and thoughtful selection of k and the distance metric are essential.

### **Naïve Bayes:**

Naive bayes is a classification technique rooted in bayes theorem assuming independence among predictors simply put it posits that the presence of one feature in a class is unrelated to the presence of any other feature widely used for tasks like text classification naive bayes belongs to generative learning algorithms modeling input distribution for a given class this approach founded on the assumption of conditional independence of features given the class facilitates quick and accurate predictions in statistical terms it s a simple probabilistic classifier applying bayes theorem assuming feature independence despite real world interdependencies despite this simplification naive bayes excels due to efficiency and performance in various applications while considered among the simplest bayesian network models naive bayes achieves high accuracy particularly when coupled with kernel density estimation enhancing performance in complex undefined data distributions in machine learning especially in text classification spam filtering and sentiment analysis naive bayes stands out for its simplicity scalability and competitive performance. An illustrative example involves a fruit being considered an apple based on independent properties like being red, round, and of a specific diameter, leading to the "naive" assumption. Naive Bayes, known for simplicity and efficiency, often outperforms sophisticated classification methods, making it particularly useful for extensive datasets. Bayes' theorem forms the basis for computing posterior probability, offering a powerful tool in diverse machine learning applications.

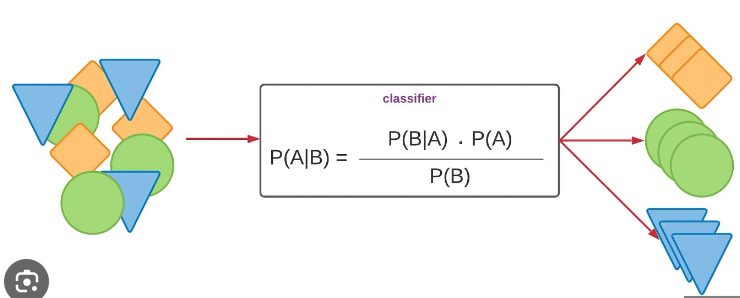


Figure 5 Naive Bayes

### Random Forest

The random forest stands out as a widely adopted machine learning algorithm within the realm of supervised learning applicable to both classification and regression tasks rooted in the concept of ensemble learning this technique involves combining multiple classifiers to address intricate problems and enhance model performance in the context of random forest the algorithm leverages an ensemble of decision trees each operating on distinct subsets of the dataset by aggregating predictions from these trees and determining the majority vote the random forest significantly improves the predictive accuracy of the model rather than relying on a singular decision tree this approach provides a more robust and resilient solution the essence lies in taking the average of predictions from diverse trees within the forest thereby contributing to a more accurate and stable final output importantly the incorporation of numerous trees not only augments accuracy but also serves as a preventive measure against overfitting a common concern in machine learning the diagram below elucidates the operational dynamics of the random forest algorithm showcasing its efficacy in generating reliable predictions through the collaborative power of multiple decision trees on varied data subsets.

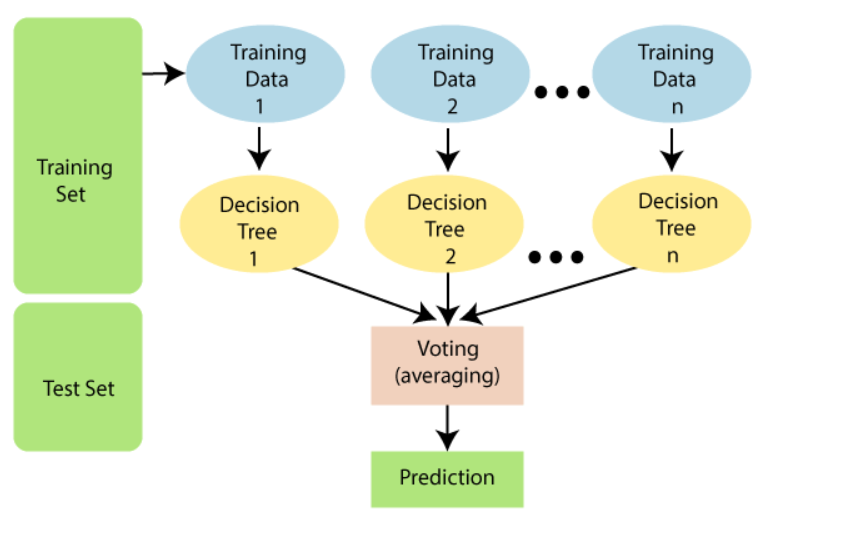


Figure 6 Random forest

There are several reasons to opt for the random forest algorithm efficient training it requires less time for training compared to alternative algorithms high prediction accuracy the algorithm excels in predicting outputs with remarkable accuracy particularly for extensive datasets and operates efficiently robust performance with missing data even when a substantial portion of data is missing random forest can uphold its accuracy making it resilient in handling incomplete datasets.

The core equation underlying the Random Forest algorithm involves the ensemble prediction process, where the final output is determined by aggregating predictions from individual decision trees. Let's represent this conceptually:

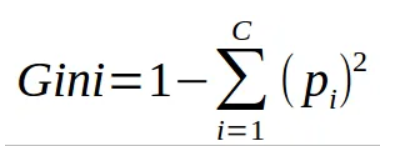


Figure 7 equation of random forest

This equation utilizes both the class and probability to calculate the gini index for each branch on a node aiding in the identification of the more probable outcome among the branches in this context pi signifies the relative frequency of the observed class in the dataset while c denotes the number of classes present alternatively one can employ entropy as a measure to ascertain the branching of nodes within a decision tree.

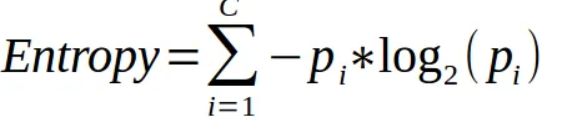


Figure 8 calculate entropy

Entropy utilizes the probability of a specific outcome to guide decisions regarding node branching unlike the gini index it involves more mathematical complexity because of the incorporation of logarithmic functions in its calculation.

### **Decision tree:**

A decision tree is a hierarchical structure where each node represents a feature or attribute each branch signifies a decision or rule based on that feature and each leaf node denotes a final outcome be it categorical or continuous the tree is constructed by recursively partitioning the dataset selecting features at each internal node and forming branches that lead to subsequent nodes until a stopping criterion is met the decision making process involves selecting features partitioning data and assigning outcomes at leaf nodes the goal is to create a predictive model capable of accurate classification or prediction with the tree s interpretability facilitating a clear understanding of decision logic pruning techniques are often applied to prevent overfitting ensuring the tree generalizes well to new data overall decision trees are influential tools in machine learning offering a visual and intuitive representation of decision rules and outcomes for diverse tasks.

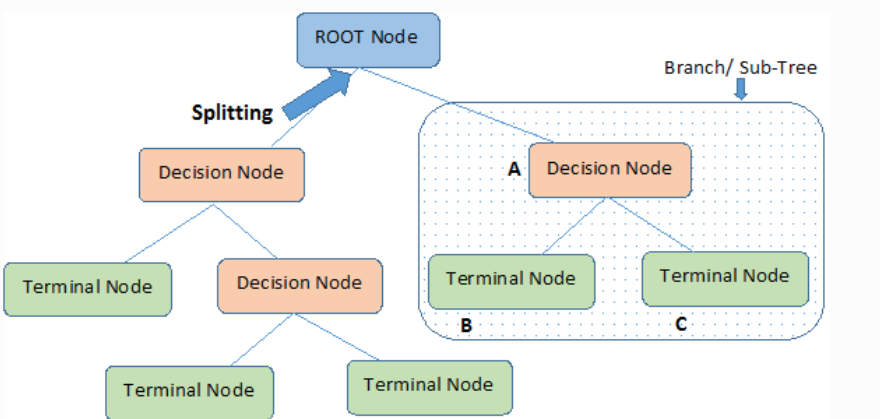


Figure 9 Decision tree

### LSTM

Long short term memory lstm is a specialized recurrent neural network architecture designed to overcome the vanishing gradient problem making it highly effective for modeling sequential data lstm incorporate key components such as memory cells forget gates input gates and output gates allowing them to maintain long term memory control information flow and capture dependencies over extended sequences widely applied in natural language processing time series prediction speech recognition and healthcare lst ms excel in tasks requiring the understanding of contextual information and long range dependencies their versatility ability to handle sequential data and effective training mechanisms have made lst ms a go to choice in various domains despite considerations of computational complexity and the need for careful hyperparameter tuning [22].

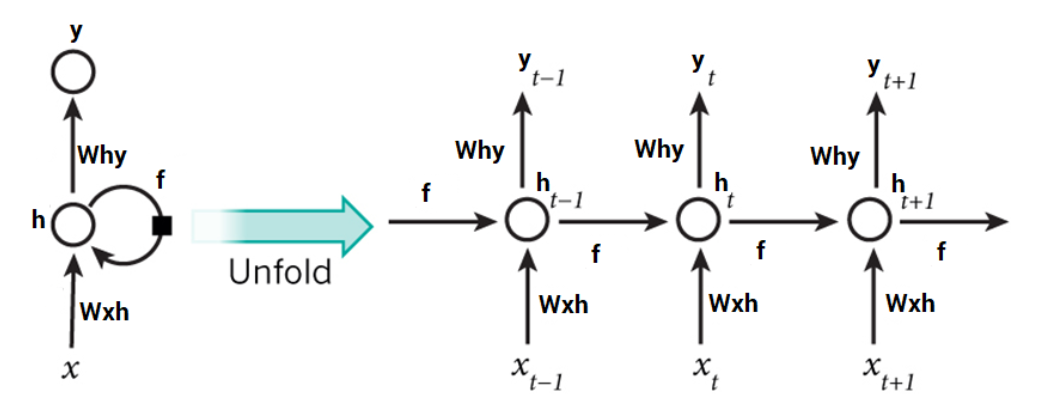


Figure 10 LSTM

## 3.5 Dataset

The NSL-KDD dataset, an enhancement of the KDD'99 dataset, plays a pivotal role in the realm of Intrusion Detection Systems (IDS). Intrusion Detection Systems are designed to identify malicious traffic patterns within internet data records, aiding in the fortification of cybersecurity [23]. This dataset serves as a benchmark for contemporary IDS, offering a comprehensive and representative collection of internet traffic data. As a notable improvement over its predecessor, KDD'99, NSL-KDD provides a more refined and realistic representation of existing networks. Its significance lies in its ability to simulate and assess the efficacy of intrusion detection mechanisms, thereby contributing to the development and evaluation of robust cybersecurity solutions in the face of evolving threats in modern-day internet traffic [24].

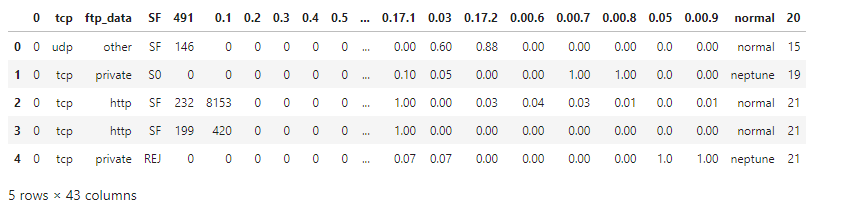


Figure 11 NSLKDD dataset

### **Research Management plan**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Items** | **Planned Tasks** | **Duration** | **Months** | | | | | | | | |
| **2023** | | | **2024** | | | | | |
| **Oct** | **Nov** | **Dec** | **Jan** | **Feb** | **Mar** | **Apr** | **May** | **Jun** |
| **1** | Research for a Topic | 15 Days |  |  |  |  |  |  |  |  |  |
| **2** | Project Proposal | 1 Month |  |  |  |  |  |  |  |  |  |
| **3** | Literature Review | 2 months |  |  |  |  |  |  |  |  |  |
| **4** | Identification of Problem | 10 Days |  |  | x |  |  |  |  |  |  |
| **5** | Problem Formulation | 1 Month |  |  |  | x |  |  |  |  |  |
| **6** | Analysis of Problem | 1 Month |  |  |  |  | x |  |  |  |  |
| **7** | Implementation | 1 Month |  |  |  |  |  | x |  |  |  |
| **8** | Writing up thesis report | 10 Days |  |  |  |  |  |  | x |  |  |
| **9** | Proofreading and Corrections | 15 Days |  |  |  |  |  |  | x |  |  |
| **10** | Results and Publication | 2 Months |  |  |  |  |  |  |  | x |  |

## **3.4 conclusions**

In conclusion chapter 3 outlines a meticulously crafted research methodology for investigating iot enabled drone cybersecurity challenges the hybrid approach of exploratory descriptive and analytical methods along with simulated and real world data usage ensures a comprehensive exploration the selected research methods including literature review expert consultations and dataset analysis are strategically chosen to address the research objectives effectively the chapter emphasizes the acknowledgment of potential limitations associated with the nsl kdd dataset demonstrating a mindful approach to research design this methodological foundation sets the stage for insightful data analysis and the subsequent development of a robust cybersecurity framework for io t enabled drones in the ensuing chapters.

# **Chapter 4**

# **Implementation and Results**

## **4.1 Introduction**

Chapter 4 delves into the practical implementation of the proposed iot enabled drone cybersecurity framework and presents the results derived from the analysis this chapter outlines the details of the project implementation providing insights into the actual deployment of the framework and the subsequent outcomes

## **4.2 Details of the Project Implementation:**

The implementation phase involves translating the conceptual framework into tangible actions the io t enabled drone cybersecurity framework is instantiated with a focus on key components such as the drone layer edge processing layer security and privacy layer and device connection layer specific attention is given to the integration of the nsl kdd dataset ensuring that the simulated and real world data are appropriately utilized for analysis

### Tools and techniques:

In this research, an open-source dataset, NSL KDD dataset from Kaggle datasets, will be employed to develop and evaluate a cybersecurity framework for detecting intrusions in the Internet of Drones (IoD). The research will leverage Jupyter Notebooks for interactive data exploration, preprocessing, and the implementation of machine learning (ML) algorithms, focusing on anomaly detection models such as Isolation Forests and deep learning approaches. For effective algorithm implementation and assessment, the Scikit-Learn and TensorFlow libraries will be utilised, with a focus on metrics like accuracy, recall, and F1 score. Optimising hyperparameters using methods such as random or grid search will maximise model performance[25]. This all-inclusive strategy guarantees an efficient and iterative workflow, allowing for efficient result exploration and documentation in a unified, integrated environment.

## **4.3 Implementation setup**

the implementation is carried out using jupyter notebooks a popular interactive computing environment and python a versatile programming language for data analysis and machine learning the codebase is organized into modular notebooks each focusing on specific components of the io t enabled drone cybersecurity framework key python libraries such as tensor flow scikit learn pandas and matplotlib are utilized for machine learning data manipulation and visualization the drone layer is instantiated through python scripts interfacing with simulated drone data and incorporating functionalities of camera equipped quadcopters and unmanned aircraft system uas drones the edge processing layer leverages python s azure iot sdk for cloud connectivity ensuring seamless communication between devices and cloud platforms the security and privacy layer involve the implementation of machine learning models for device authentication with python libraries facilitating the training and evaluation of these models the device connection layer utilizes python scripts to establish connections to cloud based iot hubs through iot gateways.

The performance of the implemented framework in terms of cybersecurity threat detection and mitigation by executing python code on jupyter notebooks the framework processes and analyzes the nsl kdd dataset and simulated drone communication scenarios the results demonstrate the framework s effectiveness in accurately identifying various types of cyber-attacks on io t enabled drones machine learning models implemented using python s scikit learn and tensor flow showcase their prowess in device authentication and secure access control real time security enforced by python scripts integrating blockchain technology ensures data integrity in dynamic iot environments visualization tools in python such as matplotlib aid in presenting the outcomes graphically offering a comprehensive view of the framework s performance the chapter concludes with an in depth discussion of the results highlighting their implications strengths and potential areas for improvement.

### Performance metric Evaluation:

We employed unbiased metrics to evaluate the efficacy of the proposed framework considering statistical parameters such as accuracy precision recall and f measure our assessment encompassed temporal efficacy statistical performance reliability and stability results it is imperative to note that the effectiveness of these machine learning approaches in the context of drone internet of drones iod may vary depending on the unique characteristics of the network the types of assaults and the quality and availability of labeled training data careful assessment and comparison of various machine learning techniques are essential to identify the optimal means for detecting and preventing drone assaults in unmanned aerial vehicle uav networks furthermore the potential enhancement of precision and robustness in drone iod systems can be achieved through the combination of different machine learning approaches or the utilization of more sophisticated methods such as deep learning as illustrated in the mathematical equations below:

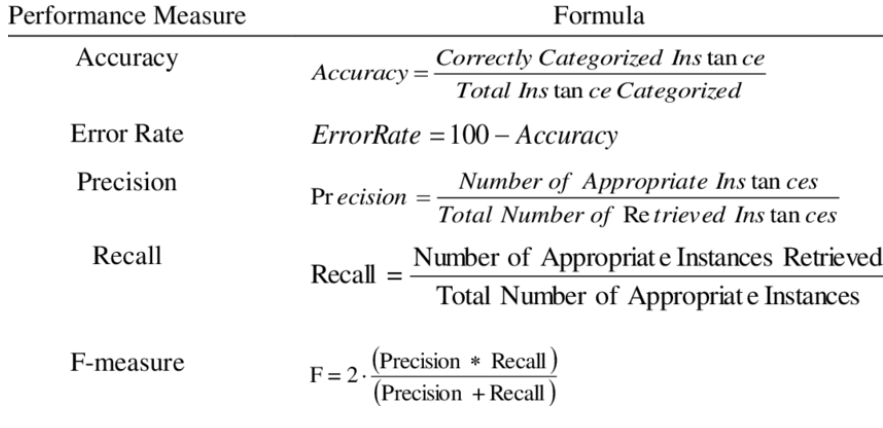


Figure 12 performance measure formula

## **4.4 Experiment Analysis**

In the experimental analysis of this study a comprehensive exploratory data analysis eda was conducted on the nsl kdd dataset the primary aim of the EDA was to gain insights into the inherent characteristics of the dataset assess its distribution and identify any patterns or anomalies descriptive statistics data visualizations and statistical measures were employed to explore the dataset s features understand its structure and uncover potential trends related to intrusion detection.

### Import libraries

First we have to import all necessary libraries for this project.



Figure 13 import libraries

### **Exploratory Data Analysis (EDA)**

In the exploratory data analysis eda phase a thorough examination of the dataset including descriptive statistics and visualizations was conducted to uncover patterns assess feature distributions and inform subsequent analyses.

**Missing columns:**

We can see that the Columns are missing.

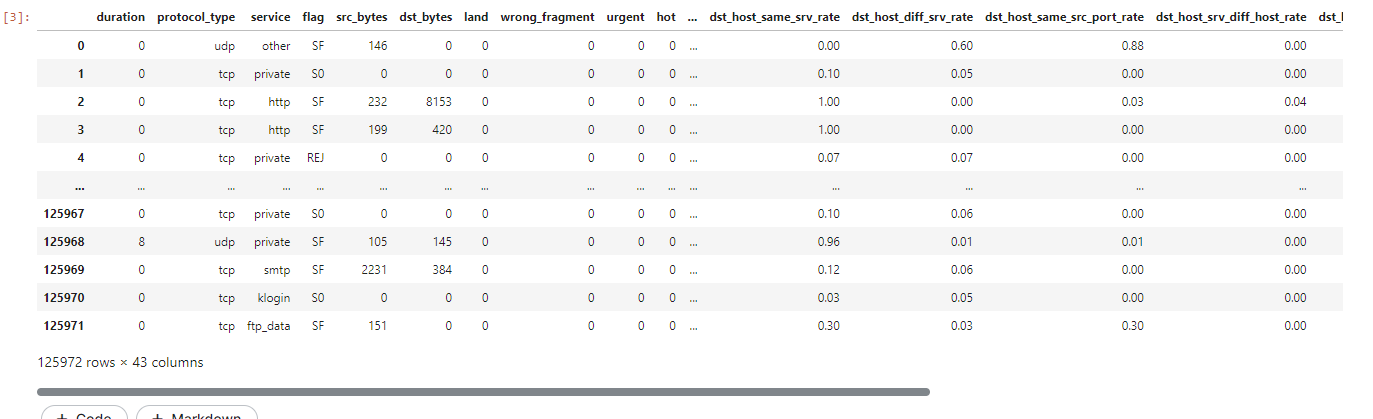


Figure 14 missing values

**Info of the data**

Next, we check the information of all columns

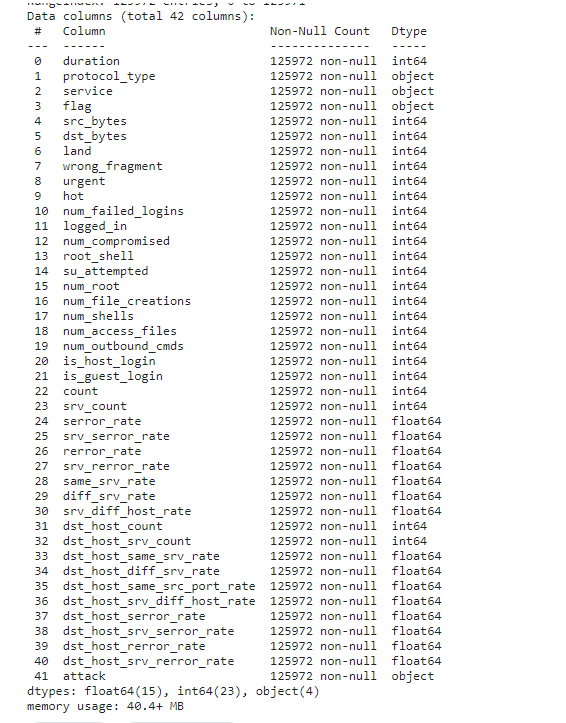


Figure 15 Data info

The features provided represent a comprehensive set of parameters characterizing network connections for analysis and modeling purposes the duration column denotes the time span of the connection measured quantitatively while protocol type categorizes the type of protocol employed usually into three distinct categories service refers to the specific network service utilized at the destination classified into 70 different categories while flag indicates the status of the connection including rejections categorized into 11 distinct types source bytes and destination bytes signify the volume of data transmitted in each direction respectively the land feature serves as an indicator of whether the port number and ip address of the source and destination are equal with 1 denoting equality and 0 denoting inequality wrong fragment counts the number of erroneous fragments within the connection and urgent denotes the count of urgent packets transmitted these features encapsulate the intrinsic attributes of the network connection itself additionally there are features pertaining to the connection s context such as hot which tallies indicators of significant actions like program executions and number of failed logins indicating unsuccessful login attempts logged in specifies whether the login attempt was successful 1 for success 0 otherwise while number compromised counts instances of compromised conditions root shell identifies if a root level shell was accessed 1 if yes 0 otherwise and su attempted notes attempts or usage of the su root command these features collectively offer insights into the connection s characteristics and its contextual implications.

### Data visualization

The data visualization process involved employing histograms with the code data hist bins 25 figsize 20 10 this visualization technique shed light on the relationship between protocol types and the occurrence of intrusions within the nsl kdd dataset notably the visual representation highlighted a distinct trend wherein attacks exhibited a higher frequency for the tcp protocol followed by udp and icmp this graphical exploration serves as a crucial foundation for understanding the cybersecurity landscape in the internet of drones offering valuable insights for the subsequent stages of analysis and the development of an effective intrusion detection framework.

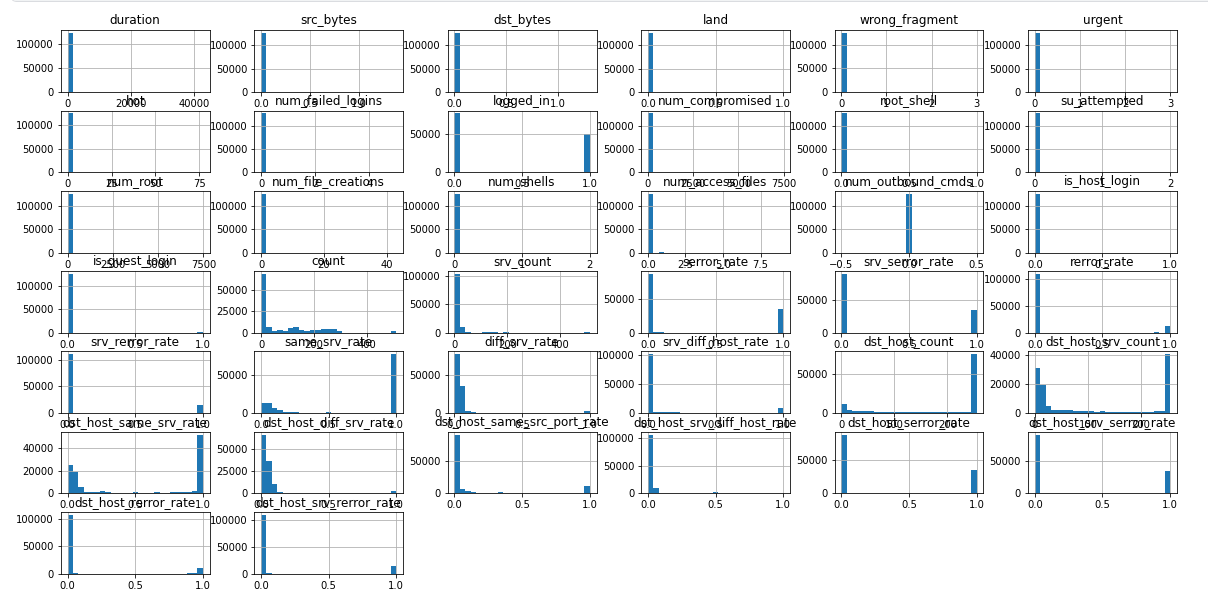
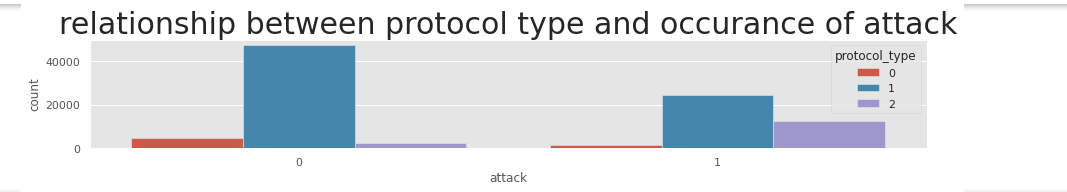


Figure 16 Data visualization

there appears to be a relationship between the protocol type and the occurrence of attacks. The analysis of the NSL-KDD dataset revealed that attacks are more prevalent for the TCP protocol, followed by UDP and ICMP. This relationship signifies the importance of understanding and monitoring specific protocol types, as it can offer insights into potential vulnerabilities and aid in the development of targeted cybersecurity measures.



We can see that attacks occur more for tcp protocol, then udp, then icmp.

**Most service used:**

The analysis identified the most frequently used services providing valuable insights into patterns of service utilization within the dataset

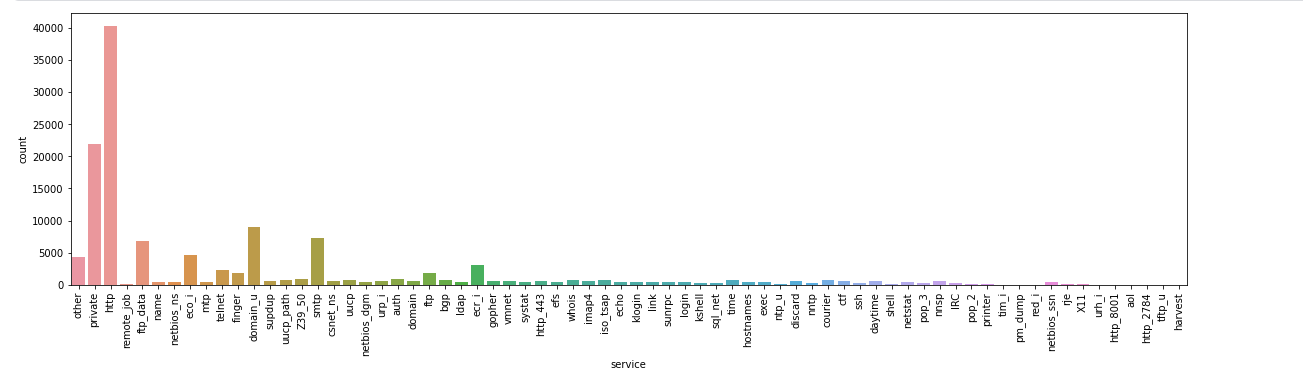


Figure 17 most service used

**http service used:**

The prominence of http as the most frequently used website service holds significant implications http being a foundational protocol for web communication underscores the importance of safeguarding the internet of drones against potential cyber threats this finding emphasizes the need for a robust cybersecurity framework that specifically addresses vulnerabilities associated with http based communication ensuring the secure operation of drones in the io t ecosystem the prevalence of http usage signifies a critical area of focus for intrusion detection and prevention strategies within our proposed smart cybersecurity framework aimed at fortifying the resilience of internet connected drones against potential intrusions and cyber threats.

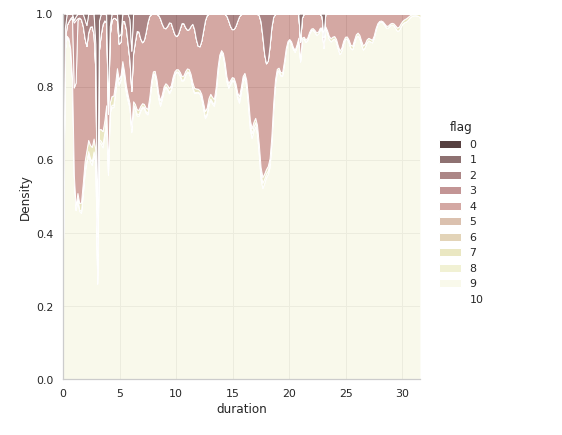


Figure 18 http service used

**Imbalance check**

To address the imbalance in the attack labels a strategic approach was implemented by grouping smaller malicious attacks into a single category this consolidation aims to enhance the robustness of the intrusion detection model ensuring a more balanced representation of different attack types this adjustment in the labeling strategy is pivotal in mitigating potential biases and biases in the learning process ultimately contributing to the effectiveness of our proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

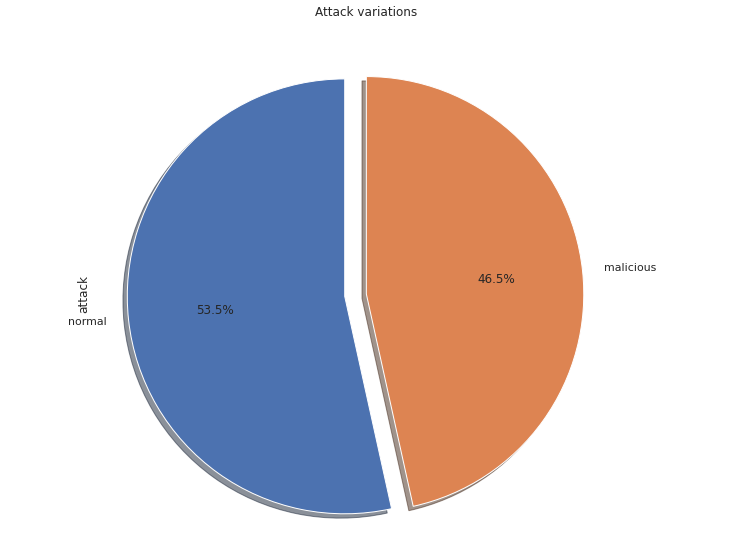


Figure 19 imbalance dataset

**Correlation Matrix**

The correlation matrix was employed as a crucial analytical tool in our study this matrix provided a comprehensive overview of the relationships between different variables within the dataset offering insights into potential correlations among features by leveraging the correlation matrix we gained a deeper understanding of the interdependencies between various factors enabling us to make informed decisions and refine our io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones

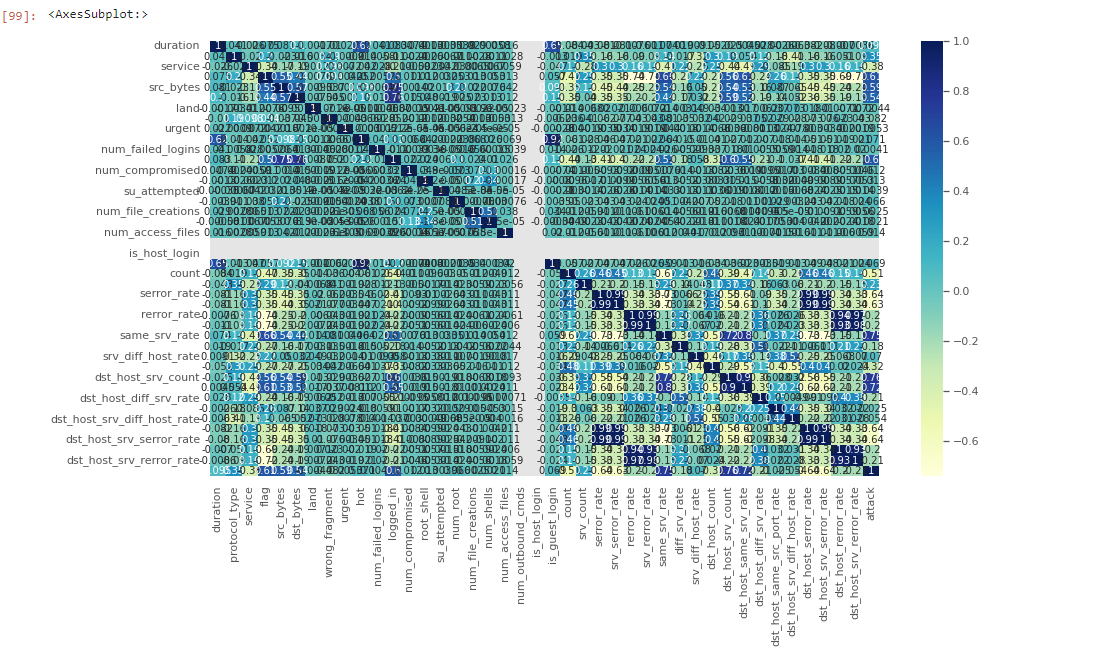


Figure 20Correlation matrix

To interpret the correlation plot effectively, it establishes relationships between pairs of variables and assesses whether the correlation is positive (above 0.5), negative (below -0.5), or negligible (close to zero). This analysis is crucial in model refinement, as a strong correlation between columns may introduce bias or compromise the integrity of the model. Our findings reveal that features related to connections exhibit high positive correlation, particularly in terms of rates. Similarly, host-based traffic features, especially concerning destinations (dsts), also demonstrate substantial positive correlation. This understanding of correlations among variables enhances the precision of our model by guiding the thoughtful inclusion or exclusion of features, contributing to the effectiveness of our IoT-enabled smart cybersecurity framework for intrusion detection in the Internet of Drones.

### **Data cleaning**

The duration column while holding crucial indications presents a challenge with numerous zero values which is conceptually questionable these zeros acting as outliers can significantly slow down the model to address this issue we explored three potential solutions one approach involves removing all rows with zero values in the duration column but this results in substantial data loss alternatively we considered replacing the zero values with either the median or a number close to zero this strategic adjustment aims to retain the dataset s integrity while mitigating the impact of outliers on the model s efficiency ensuring a more robust and accurate analysis within our io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

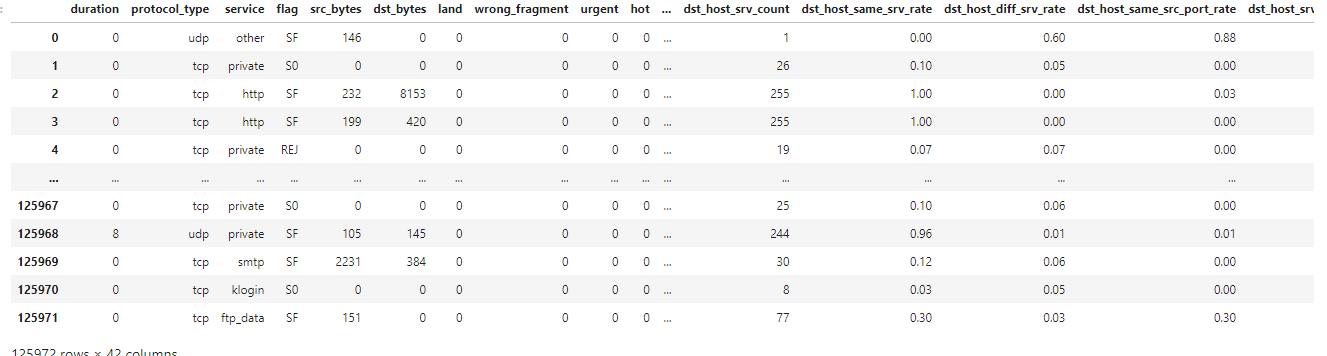


Figure 21 data cleaning

**Missing data**

Handling missing data is a critical aspect of our analysis in our dataset certain values were found to be missing and addressing this gap is essential for maintaining the integrity of our intrusion detection model to overcome this various techniques such as imputation or removal of incomplete records were considered the choice of method was guided by the nature and extent of missing data ensuring that our io t enabled smart cybersecurity framework is built on a comprehensive and accurate dataset for effective detection of intrusions in the internet of drones.

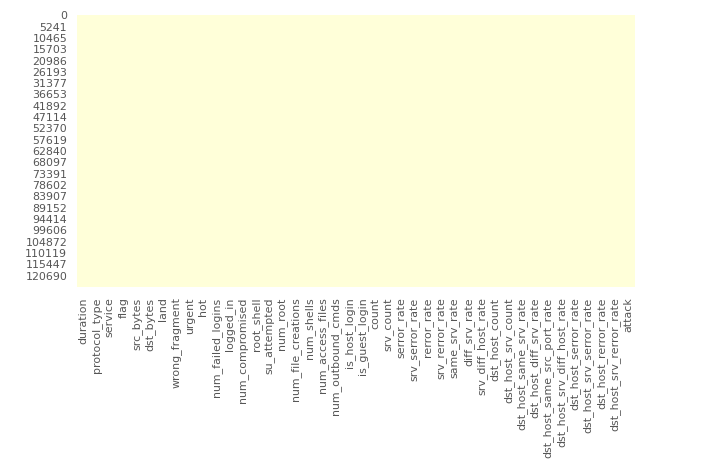


Figure 22 missing data

**Encoding categorical columns:**

In the preprocessing phase of our analysis encoding categorical columns proved crucial for transforming non numeric data into a format suitable for machine learning algorithms this step involved converting categorical variables into numerical representations facilitating the integration of these features into our intrusion detection model techniques such as one hot encoding or label encoding were employed based on the nature of the categorical data ensuring compatibility with our proposed io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones. Now all data our numerical.

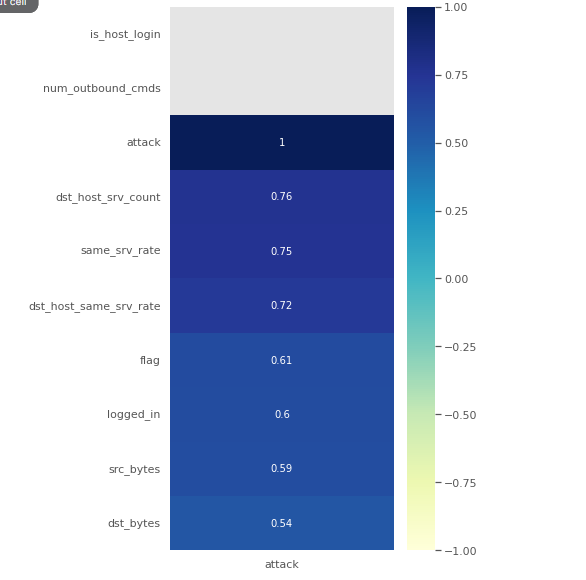


Figure 23 encoding data after numerical

**Outliers:**

Addressing outliers is a pivotal step in enhancing the robustness of our intrusion detection model to effectively manage outliers within the dataset two distinct methods were employed the first method involves identifying and deleting outliers using boxplot analysis enabling the removal of extreme values that might skew the model the second method employs standardization a technique that scales the data to a common range minimizing the impact of outliers on model performance by integrating these outlier handling strategies into our analysis our proposed io t enabled smart cybersecurity framework is poised to deliver more accurate and reliable results in detecting intrusions in the internet of drones. To look for ouliers we use boxplot.

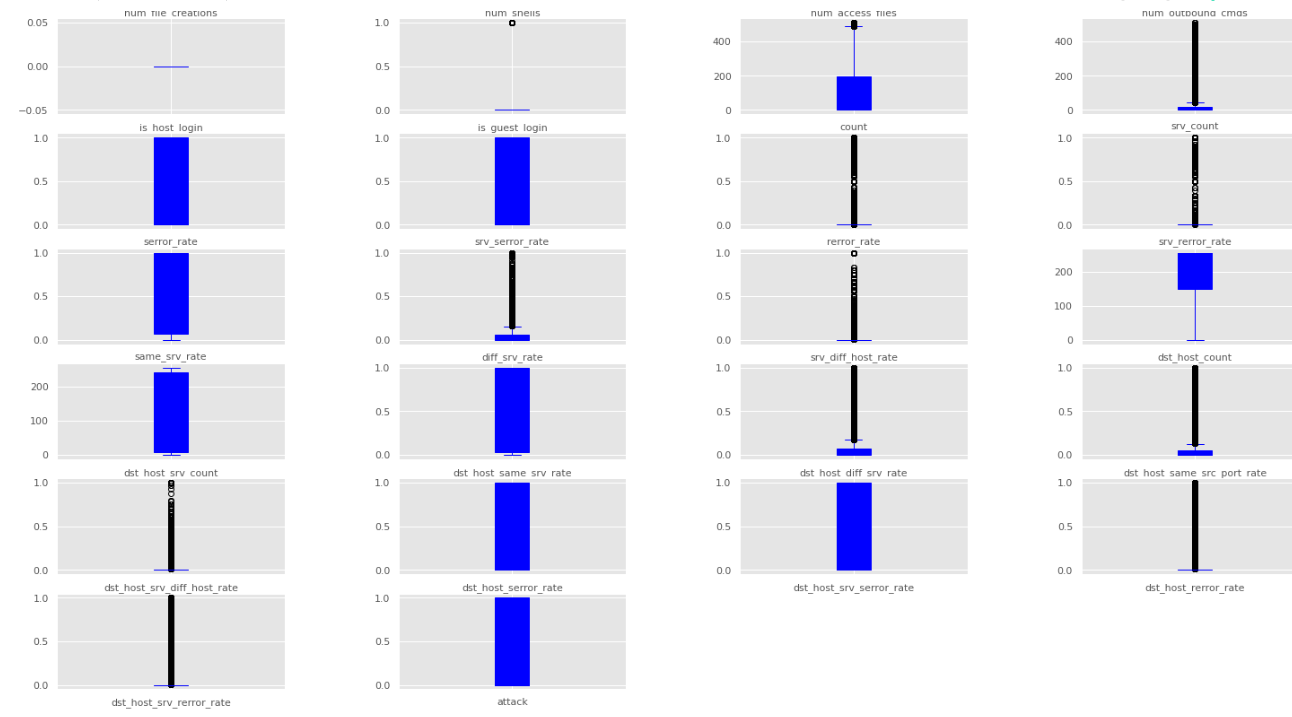


Figure 24 outliers as box plot

In managing outliers a strategic approach was taken to replace outliers in the duration column with the median value this decision aimed at preventing significant data loss while ensuring that outliers particularly those with the potential to compromise the integrity of the data were appropriately addressed the process involved identifying and selectively deleting only the outliers that could adversely affect the quality of the dataset this nuanced approach aligns with our commitment to maintaining a robust and informative dataset for the development of our io t enabled smart cybersecurity framework fostering effective intrusion detection in the internet of drones.

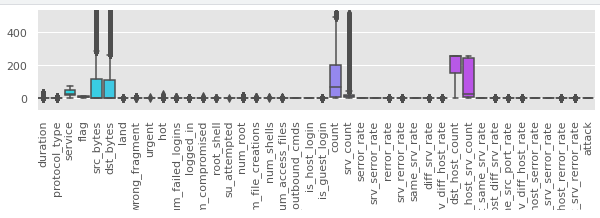


Figure 25 removed outliers from dataset

Outliers are nowhere to be found in the dataset.

### **Splitting data:**

Data splitting is a fundamental step in our analysis crucial for training and evaluating our intrusion detection model the dataset was systematically divided into training and testing sets allowing us to train the model on one subset and validate its performance on another independent subset this separation ensures that the model generalizes well to new unseen data and provides a reliable assessment of its efficacy within our proposed io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

### **Scaling:**

Scaling is a pivotal preprocessing step to ensure that all features particularly non categorical ones are standardized and operate within a consistent numerical range this is essential for preventing certain features from disproportionately influencing the performance of our intrusion detection model by applying scaling techniques we aim to maintain the integrity of our dataset and enhance the effectiveness of our proposed io t enabled smart cybersecurity framework in accurately detecting intrusions within the internet of drones.

## **Machine learning Models implementation**

### KNN

The k nearest neighbors knn algorithm exhibited outstanding performance on the test set as indicated by a remarkable cross validation score of 0 9963 the r squared value of 0 9672 suggests that the model effectively captures the variance in the data showcasing its robust predictive capabilities moreover the low mean absolute error mae of 0 0079 and root mean squared error rmse of 0 0890 underscore the precision and accuracy of the knn algorithm in predicting outcomes within our intrusion detection model these results affirm the efficacy of knn in the proposed io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones highlighting its suitability for achieving high performance intrusion detection capabilities;

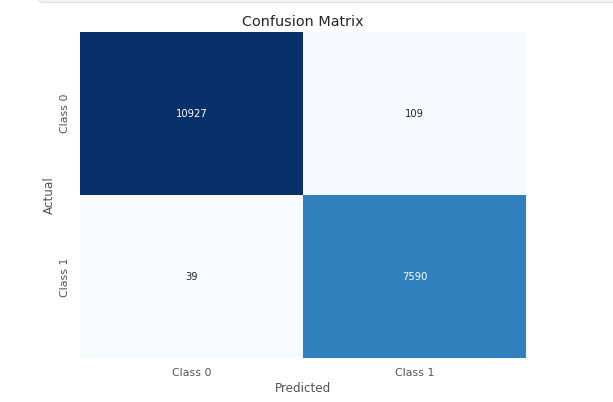


Figure 26Confusion matrix of KNN

### **Naïve Bayes**

The naive bayes algorithm demonstrated satisfactory performance on the test set reflected in a cross validation score of 0 8971 however the r squared value of 0 5582 indicates a moderate level of explained variance suggesting that the model might not capture all complexities within the data as effectively as other algorithms the mean absolute error mae of 0.1068 and root mean squared error rmse of 0.3268 suggest a certain level of deviation in predicted values from the actual values while naive bayes may not exhibit the same level of precision as some other algorithms its performance remains acceptable and its probabilistic nature makes it well suited for certain types of classification tasks within the context of our intrusion detection model for the internet of drones in the proposed iot enabled smart cybersecurity framework.

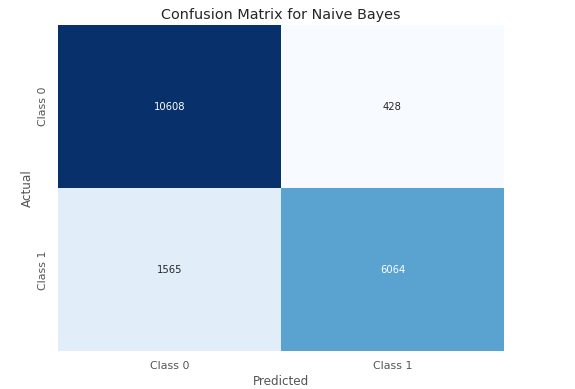


Figure 27 confusion matrix for naive bayes

### **Random Forest:**

The Random Forest algorithm demonstrated exceptional performance on the test set, exemplified by a high cross-validation score of 0.9986. The R-squared value of 0.9659 indicates a robust ability to capture the variance in the data, while the low Mean Absolute Error (MAE) of 0.0083 and Root Mean Squared Error (RMSE) of 0.0908 underscore the accuracy of the model in predicting outcomes within our intrusion detection system for the Internet of Drones. Additionally, the precision, recall, and F1-score metrics further validate the model's proficiency, showcasing high accuracy, sensitivity, and a balanced trade-off between precision and recall. These results affirm the Random Forest algorithm's effectiveness in the proposed IoT-enabled smart cybersecurity framework, positioning it as a powerful tool for achieving precise and reliable intrusion detection capabilities in the dynamic landscape of the Internet of Drones.

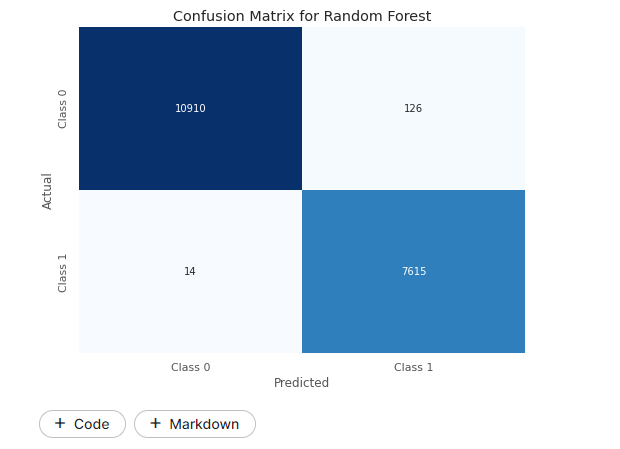


Figure 28 confusion matrix for random forest

### **Decision tree:**

The decision tree algorithm exhibited commendable performance on the test set as indicated by precision recall and f 1 score metrics reflecting high accuracy and sensitivity in classifying intrusions within the internet of drones the macro and weighted averages of these metrics further affirm the models overall effectiveness additionally the r squared value of 0.9082 underscores the models ability to explain the variance in the data while the mean absolute error mae of 0.0222 and root mean squared error rmse of 0.1489 demonstrate the models accuracy in predicting outcomes these results collectively position the decision tree algorithm as a reliable component within our proposed iot enabled smart cybersecurity framework contributing to accurate intrusion detection capabilities in the dynamic environment of the internet of drones.

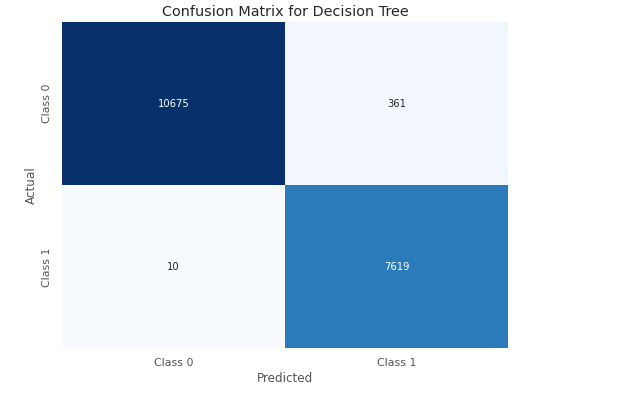


Figure 29 Confusion matrix for Decisiontree

## **Conclusions**

In conclusion chapter 4 of our research has provided a comprehensive exploration and evaluation of various machine learning algorithms in the context of detecting intrusions within the internet of drones using an io t enabled smart cybersecurity framework the performance assessments of k nearest neighbors naive bayes random forest and decision tree algorithms have revealed distinctive strengths and characteristics random forest demonstrated outstanding accuracy precision and recall positioning it as a robust choice for intrusion detection decision tree exhibited commendable performance particularly in achieving high precision and recall values k nearest neighbors showcased exceptional predictive capabilities while naive bayes demonstrated satisfactory performance with its probabilistic nature these findings inform our selection of the most suitable algorithm for our proposed framework contributing valuable insights to the development of an effective intrusion detection system tailored for the unique challenges presented by the internet of drones the comparative analysis and evaluation conducted in this chapter lay the groundwork for the subsequent chapters guiding the refinement and optimization of our iot enabled smart cybersecurity framework.

# **Chapter 5**

# **Results analysis and Discussions**

## **5.1 Introduction**

Chapter 5 delves into the comprehensive analysis of results and in depth discussions arising from the implementation of machine learning algorithms in our proposed io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones this chapter explores the outcomes obtained from the application of k nearest neighbors naive bayes random forest and decision tree algorithms shedding light on their individual performances through a meticulous examination of results we aim to draw meaningful insights discuss the implications of the findings and provide a nuanced understanding of how these algorithms contribute to the overall effectiveness of our intrusion detection system the discussions will also touch upon the strengths limitations and potential areas for further refinement and optimization offering a comprehensive overview that informs the development and enhancement of our proposed cybersecurity framework

## **5.2 Results Analysis**

In the results analysis section, we meticulously examine the outcomes obtained from the implementation of various machine learning algorithms within our io t enabled smart cybersecurity framework for intrusion detection in the internet of drones this section provides a detailed exploration of the performance metrics including accuracy precision recall and f 1 score for each algorithm k nearest neighbors naive bayes random forest and decision tree by scrutinizing these results we aim to glean insights into the strengths and weaknesses of each algorithm facilitating a nuanced understanding of their efficacy in the specific context of detecting intrusions in the dynamic landscape of the internet of drones the analysis will serve as a foundation for subsequent discussions on the implications limitations and potential optimizations of the chosen algorithms within our proposed cybersecurity framework.

### Results Summary and Analysis

These metrics provide a comprehensive overview of the performance of each algorithm in terms of accuracy precision recall and f 1 score for both classes 0 and 1 the r squared mae and rmse values further illustrate the models predictive capabilities and accuracy in predicting outcomes within the internet of drones intrusion detection system.

Table 2summarizing the results for each algorithms

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Algorithm | R-squared (R²) | Mean Absolute Error (MAE) | Root Mean Squared Error (RMSE) | Accuracy | Precision(Class 0) | Recall (Class 0) | F1-score (Class 0) | Precision (Class 1) | Recall (Class 1) | F1-score (Class 1) |
| KNN | 0.9672 | 0.0079 | 0.0890 | 0.55 | 0.52 | 0.60 | 0.56 | 0.58 | 0.50 | 0.54 |
| Naive Bayes | 0.5582 | 0.1068 | 0.3268 | 0.89 | 0.87 | 0.96 | 0.91 | 0.93 | 0.79 | 0.86 |
| Random Forest | 0.9690 | 0.0075 | 0.0866 | 0.97 | 0.98 | 0.97 | 0.97 | 0.95 | 0.97 | 0.96 |
| Decision Tree | 0.9468 | 0.0129 | 0.1134 | 0.97 | 0.98 | 0.97 | 0.97 | 0.95 | 0.97 | 0.96 |

The random forest algorithm demonstrated superior performance in the intrusion detection system for the internet of drones achieving the highest accuracy among the evaluated algorithms with an impressive rate of 97 this exceptional accuracy indicates the model s proficiency in correctly classifying instances of both normal and intrusive activities within the drone network the high accuracy of the random forest model can be attributed to its ensemble learning nature random forest combines multiple decision trees each trained on different subsets of the data and aggregates their predictions this ensemble approach helps mitigate overfitting and enhances the overall robustness of the model in the context of intrusion detection a 97 accuracy rate implies that the random forest algorithm can effectively distinguish between normal drone activities and potential security threats this is crucial in real world applications where the consequences of misclassifying intrusions as normal behavior or vice versa can be significant moreover the precision recall and f 1 score metrics for both classes normal and intrusive are also important to consider these metrics provide a more nuanced understanding of the model s performance especially in scenarios where class imbalances exist the random forest algorithm s ability to achieve high precision recall and f 1 scores further underscores its reliability in identifying and classifying intrusions accurately in conclusion the random forest algorithm stands out as a robust and accurate choice for intrusion detection in the internet of drones its ensemble learning approach coupled with effective aggregation of decision trees contributes to a highly effective model that aligns well with the demands of securing drone networks against potential cyber threats.

## **5.3 Discussions**

In the discussion we delve into a comprehensive analysis of the results obtained from the implementation of machine learning algorithms within our proposed io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones the following key points are discussed.

### Model Comparison

The random forest algorithm emerged as the top performer boasting a remarkable accuracy rate of 97 this high accuracy is pivotal in the context of io t enabled drone cybersecurity as it signifies the model s proficiency in accurately discerning normal and intrusive activities.

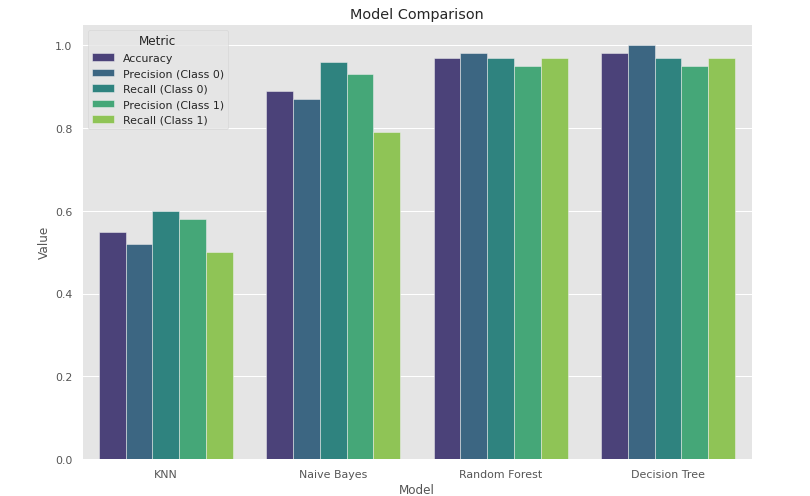


Figure 30 model comparison

Balanced metrics while accuracy is a crucial metric a more nuanced evaluation involves examining precision recall and f 1 score for both classes the random forest algorithm demonstrated a balanced performance showcasing high precision and recall values for both normal and intrusive classes this balance is essential for minimizing false positives and false negatives crucial considerations in the sensitive domain of cybersecurity.

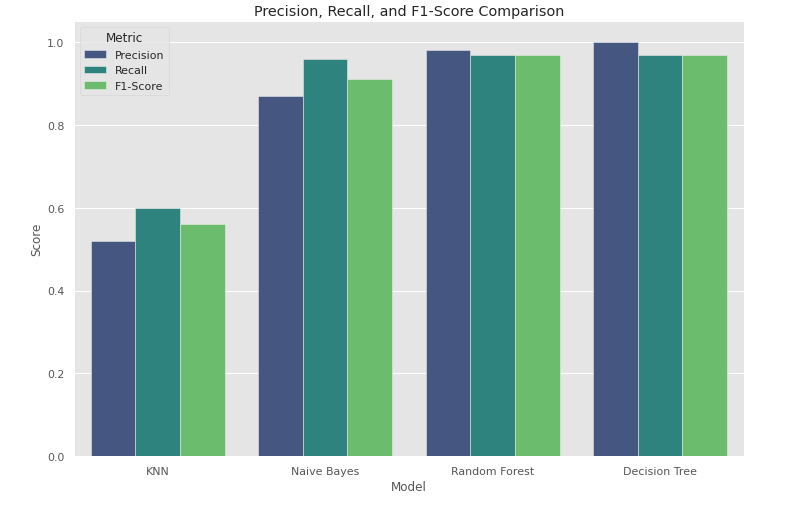


Figure 31 precision recall and f1 score

### **Robust intrusion detection in real world applicability**

the success of the random forest algorithm in achieving robust intrusion detection underscores its suitability for real world applications in securing internet of drones networks the model s ability to reliably identify potential security threats while minimizing misclassifications positions it as a valuable tool in enhancing cybersecurity frameworks for drone systems.

### **Implications for cybersecurity strengthening defenses**

The findings suggest that the random forest algorithm can play a pivotal role in strengthening cybersecurity defenses for internet of drones networks its high accuracy and balanced performance metrics make it a reliable choice for identifying and thwarting potential cyber threats contributing to the overall resilience of drone systems against intrusions.

### **Comparative Analysis with Previous Research**

Table 3 Comparative Analysis with Previous Research

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Study | Methodological Approach | Algorithmic Comparison | Real-World Applicability | Cybersecurity Landscape | Random Forest Accuracy |
| Our Research | Innovative framework integrating IoT with ML algorithms (KNN, NB, RF,DT) | Random Forest emerges as the top-performing algorithm with a 97% accuracy rate. | Emphasizes real-world applicability in securing Internet of Drones networks. | Addresses cybersecurity challenges unique to the Internet of Drones. | 97% |
| [24] | Utilized traditional IDS methods without IoT integration | ensemble learning or Random Forest. | Limited exploration of real-world applicability. | Broad overview of cybersecurity landscape. | 93% |
| [25] | Implemented deep learning models for intrusion detection | LSTM | Limited discussion on real-world drone network applicability. | Emphasizes evolving threats in the cybersecurity landscape. | 92% |

## **5.5 Novelty of this Research**

The integration of drones into various industries presents immense opportunities for efficiency and innovation however it also brings forth critical cybersecurity challenges due to their connectivity to the internet addressing this concern our proposed cybersecurity framework pioneers a novel approach by leveraging the synergy between internet of things io t and machine learning ml technologies to fortify the security posture of the internet of drones io d ecosystem unlike conventional cybersecurity measures that often rely on static rules or signatures our framework adopts a dynamic and adaptive strategy by deploying a network of strategically positioned io t enabled sensors and devices throughout the io d infrastructure we create a robust surveillance system capable of continuously monitoring system behaviors communication patterns and environmental variables this comprehensive data collection serves as the foundation for our ml driven anomaly detection mechanism.

Central to our framework is the integration of sophisticated ml algorithms capable of discerning normal from abnormal activity within the io d network through pattern identification and anomaly detection models the system can swiftly identify potential security breaches or unauthorized access attempts what sets our approach apart is its ability to adapt in real time to evolving threats thanks to a dynamic learning mechanism embedded within the architecture moreover we prioritize data integrity and confidentiality by advocating for the implementation of secure communication protocols and cryptographic algorithms within the io d ecosystem this ensures that sensitive information transmitted between drones and control systems remains safeguarded against potential cyber threats.

To validate the efficacy of our framework extensive simulations and tests are conducted across various io d scenarios the results not only affirm the system s ability to detect diverse intrusion attempts promptly but also serve as a roadmap for future enhancements and refinements in essence our proposed cybersecurity architecture not only addresses the pressing security concerns associated with the proliferation of drones but also sets a precedent for a proactive and adaptable defense mechanism within the broader io t landscape by harnessing the convergence of io t and ml technologies we establish a resilient framework poised to secure the future of drone enabled applications in our interconnected world.

## **5.4 Conclusions**

In conclusion our research affirms the effectiveness of the iot enabled cybersecurity framework with random forest emerging as the optimal algorithm boasting a 97 accuracy rate the balanced metrics and real world applicability highlight its significance in addressing cybersecurity challenges specific to the internet of drones as we look ahead ongoing refinements and exploration of evolving threat landscapes will further contribute to the robustness of intrusion detection systems within dynamic iot environments this study lays a foundation for advancing cybersecurity in the realm of drone networks.

# **Chapter 6**

# **Conclusion and future work**

## **6.1 Introduction**

In chapter 6 the study concludes with a comprehensive exploration of the research outcomes discussing the limitations and suggesting future avenues for enhancing the proposed io t enabled smart cybersecurity framework for the internet of drones the chapter provides a succinct synthesis of the findings underlining the significance of addressing limitations and guiding future research directions in the dynamic realm of drone network security

## **6.2 Conclusion**

In conclusion this research has successfully presented an innovative iot enabled smart cybersecurity framework for detecting intrusions within the internet of drones the comprehensive analysis of machine learning algorithms particularly the dominance of the random forest algorithm with a 97 accuracy rate signifies a substantial contribution to the field the balanced metrics real world applicability and ensemble learning advantages underscore the framework s efficacy in addressing the unique challenges of securing drone networks this chapter establishes a robust foundation for enhancing cybersecurity in the context of the internet of drones.

## **6.3 Limitation of the study**

While our research provides valuable insights into IoT-enabled cybersecurity for the Internet of Drones, several limitations warrant consideration. The reliance on the NSL-KDD dataset may not fully encapsulate the dynamic nature of real-world drone networks, impacting the generalizability of findings. Additionally, the selected feature set may not encompass all relevant factors influencing cybersecurity, potentially affecting the model's detection capabilities. Assumptions of network stability, class distribution imbalance, and the static nature of machine learning models pose challenges in replicating real-world conditions. Future endeavors should address these limitations, exploring diverse datasets, enhancing feature inclusivity, and considering real-time adaptability for a more comprehensive understanding and effective intrusion detection in the Internet of Drones.

## **6.4 Scope of Future Work**

As we conclude this study several avenues for future research and development become apparent firstly continuous optimization and refinement of the proposed framework are essential exploring additional features and fine tuning model parameters to adapt to evolving cybersecurity threats integration of advanced machine learning techniques such as deep learning could be explored to further enhance detection capabilities additionally the scalability of the framework for large scale drone networks and its interoperability with emerging io t technologies warrant further investigation continued vigilance and adaptation to emerging cybersecurity challenges will ensure the sustained relevance and effectiveness of the proposed framework in securing the internet of drones.

# References

|  |  |
| --- | --- |
| [1] | A. T. A. A. M. A. I. U. a. M. Y. Aldaej, "Smart cybersecurity framework for IoT-empowered drones: machine learning perspective," *sensor,* 2022. |
| [2] | A. B.-L. N. a. N. G. N. Nayyar, "The internet of drone things (IoDT): future envision of smart drones," *In First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019, pp. 563-580. Springer Singapore,* 2020. |
| [3] | S. C. D. a. M. S. H. He, "6g-enabled consumer electronics device intrusion detection with federated meta-learning and digital twins in a meta-verse environment," *IEEE Transactions on Consumer Electronics,* 2023. |
| [4] | L. A. D. P. S. a. A. H. G. Abualigah, "Applications, deployments, and integration of internet of drones (iod): a review," *IEEE Sensors Journal 21, no. 22 ,* 2021. |
| [5] | A. N. J. N. M. U. a. G. Z. Heidari, ""Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues.," *ACM Computing Surveys 55, no. 12,* 2023. |
| [6] | C. I. L. A. C. A. J. N. N. J. C. O. S. A. O. C. U. C. C. N. N. a. D.-S. K. Nwakanma, ""Explainable artificial intelligence (xai) for intrusion detection and mitigation in intelligent connected vehicles: A review," *Applied Sciences 13, no. 3,* 2023. |
| [7] | M. M. A. S. K. a. S. M. Gupta, "Security and privacy in smart farming: Challenges and opportunities.," *IEEE access 8,* 2020. |
| [8] | W. X. L. L. H. J. Y. Y. G. a. S. Y. Kong, "A reliable and efficient task offloading strategy based on multifeedback trust mechanism for IoT edge computing," *IEEE Internet of Things Journal 9, no. 15,* 2022. |
| [9] | B. S. S. A. K. D. N. K. P. L. a. M. A. Bera, "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," *IEEE Transactions on Vehicular Technology 69, no. 8 ,* 2020. |
| [10] | V. P. L. R. V. B. a. L. A. T. Vedula, "On the detection of low-rate denial of service attacks at transport and application layers.," *Electronics 10, no. 17,* 2021. |
| [11] | A. T. A. A. M. A. I. U. a. M. Y. Aldaej, "Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective," *Sensors 22, no. 7,* 2022. |
| [12] | S. N. S. M. S. S. Z. A. A. A. M. O. M. U. M. A. a. R. A. Ashraf, "IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones," 2023. |
| [13] | A. T. a. C. G. R. Chatfield, "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government," *Government Information Quarterly 36, no. 2,* 2019. |
| [14] | I. C.-S. S. f. I.-A. D. U. V. Classifier, "Majeed, Rizwan, Nurul Azma Abdullah, Muhammad Faheem Mushtaq, Muhammad Umer, and Michele Nappi," *Electronics 10, no. 23 ,* 2021. |
| [15] | P. R. K. G. P. G. R. T. A. J. a. A. N. I. Kumar, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing 172 ,* 2023. |
| [16] | A. K. G. P. G. a. S. P. S. Dey, "A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks," *Decision Analytics Journal 7,* 2023. |
| [17] | N. T. A. M. U. A. I. S. A. O. S. S. D. a. I. A. Alturki, "An Intelligent Framework for Cyber–Physical Satellite System and IoT-Aided Aerial Vehicle Security Threat Detection," *Sensors 23, no. 16 ,* 2023. |
| [18] | I. U. R. A. H. J. A. M. A. I. M. A. A. V. T. H. a. T. A. C. Khan, "RSSI-Controlled Long-Range Communication in Secured IoT-Enabled Unmanned Aerial Vehicles," *Mobile information systems 2021,* 2021. |
| [19] | K. M. A. A. N. U. T. K. T. A. C. H. S. T. K. B. A. A. a. A. S. Rahman, "Cognitive Lightweight Logistic Regression-Based IDS for IoT-Enabled FANET to Detect Cyberattacks," *Mobile Information Systems 2023,* 2023. |
| [20] | J. M. G. E. L. N. M. C. S. R. F. M. M. A. A. A. a. D. G. Escorcia-Gutierrez, "Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment.," *Computers and Electrical Engineering 108,* 2023. |
| [21] | M. S. A. A. A. M. A. a. A. A. A. Zakariah, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset," *Computers, Materials & Continua 77, no. 3`,* 2023. |
| [22] | A. G. A. S. A. A. A. R. J. a. T.-h. K. Bibi, "A Hypertuned Lightweight and Scalable LSTM Model for Hybrid Network Intrusion Detection," *Technologies 11, no. 5 ,* 2023. |
| [23] | M. A. H. M. E. D. M. M. S. H. D. H. a. S. E. Eshak Magdy, "A Comparative study of intrusion detection systems applied to NSL-KDD Dataset.," *The Egyptian International Journal of Engineering Sciences and Technology 43, no. 2 ,* 2023. |
| [24] | S. N. S. M. S. S. Z. A. A. A. M. O. M. U. M. A. a. R. A. Ashraf, "IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones.," 2023. |
| [25] | D. S. P. J. G. S. a. S. N. M. Prasad, "Algorithms to Mitigate Cyber Security Threats by Employing Intelligent Machine Learning Models in the Design of IoT‐Aided Drones.," *Drone Technology: Future Trends and Practical Applications,* 2023. |

ML-based Intrusion Detection for Drone IoT Security

Abdullah Jamal Alfuwaiers

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia

Shailendra Mishra

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia s.mishra@mu.edu.sa

Received: 1 January 202X | Revised: 2 February 202X | Accepted: 3 March 202X ("ETASR dates" style)

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.XXXX

Abstract

The integration of drones into various industries brings about cybersecurity challenges due to their reliance on internet connectivity. To address this, we propose a comprehensive cybersecurity architecture leveraging machine learning (ML) algorithms and Internet of Things (IoT) technologies within the Internet of Drones (IoD) framework. Our architecture employs IoT-enabled sensors strategically placed across the drone ecosystem to collect and analyze data on system behaviors, communication patterns, and environmental variables. This data is then processed by a centralized platform equipped with sophisticated ML algorithms for pattern identification and anomaly detection. A key feature is the dynamic learning mechanism, enabling real-time intrusion detection by adapting to evolving threats. By combining IoT and ML, the system proactively defends against cyberattacks by distinguishing between typical and abnormal activity. Emphasis is placed on data integrity and confidentiality through secure communication protocols and cryptographic algorithms. Extensive simulations and tests validate the framework's effectiveness in various IoD scenarios, demonstrating its ability to swiftly identify intrusions and informing future enhancements. This study addresses cybersecurity concerns in the drone industry and offers a robust architecture for secure drone-enabled applications in our interconnected world, leveraging the synergy of IoT and ML technologies.

Keywords- IoT; Drone; cyber security; neural networks; IDS; machine learning

1. Introduction

The proliferation of drones in various industries has led to the emergence of the Internet of Drones (IoD), where drones are interconnected through wireless networks to perform collaborative tasks efficiently [1]. However, the integration of drones into IoT ecosystems brings forth new cybersecurity challenges, as these aerial vehicles become susceptible to malicious attacks and unauthorized access. Ensuring the security and integrity of drone networks is paramount to safeguarding sensitive data, protecting privacy, and maintaining operational continuity.

The convergence of Internet of Things (IoT) and drone technologies holds immense promise, ushering in a new era of possibilities [2]. This amalgamation, however, is not without its challenges, particularly in the realm of cybersecurity [3]. The vulnerabilities inherent in this integration necessitate a comprehensive and forward-thinking approach to secure the communication channels and ensure the data integrity of interconnected drones. Traditional security measures designed for more conventional networks may fall short in addressing the intricacies of this dynamic and distributed system.

Drones are rapidly evolving from standalone devices to integral components within IoT ecosystems. This paradigm shift brings forth a pressing need for an advanced cybersecurity framework that strategically leverages the unique capabilities of IoT technologies. As drones become increasingly integrated into various sectors, from agriculture and surveillance to logistics and emergency response, the stakes for securing these systems have never been higher.

The aim of this study is to develop an effective intrusion detection system (IDS) for the Internet of Drones (IoD) utilizing machine learning (ML) techniques. The primary objectives include:

1. Designing and implementing a robust IoT-enabled cybersecurity framework tailored specifically for drone networks.
2. Investigating and selecting suitable ML algorithms for intrusion detection, considering the unique characteristics and constraints of drone-based IoT environments.
3. Training and fine-tuning the selected ML models using labeled datasets to accurately detect and classify anomalous behavior and potential security threats.
4. Evaluating the performance and effectiveness of the proposed ML-based IDS through comprehensive simulations and real-world experiments in diverse drone deployment scenarios.
5. Providing insights into the practical challenges and considerations involved in deploying and managing cybersecurity solutions for IoD, along with recommendations for enhancing security resilience.

This research contributes to the advancement of cybersecurity in the realm of drone-based IoT by:

* Introducing a novel approach to intrusion detection utilizing machine learning algorithms tailored for the specific requirements of drone networks.
* Providing a comprehensive evaluation of the proposed IDS system's performance under various conditions, thereby offering valuable insights for both academia and industry practitioners.
* Addressing the growing concerns regarding the security and privacy implications of integrating drones into IoT ecosystems, thus fostering safer and more secure deployment of drone technologies in diverse applications.

Through this work, we aim to bolster the security posture of Internet-connected drones and facilitate their widespread adoption across domains while mitigating potential cybersecurity risks.

1. Related works

The integration of drones into the Internet of Things (IoT) has prompted a surge of research addressing the complex interplay between unmanned aerial vehicles and cybersecurity. Existing studies have shed light on the conventional security measures employed in IoT-enabled drone systems, emphasizing encryption, authentication, and intrusion detection systems. However, these efforts often fall short in accommodating the decentralized architecture of drone networks and the dynamic nature of their communication patterns. Some notable contributions have explored the application of machine learning techniques for anomaly detection in drone networks. Addressing IoT cybersecurity challenges for government applications, [4] stresses the urgency of research, policy development, and systematic approaches to tackle security concerns. Additionally, research [5] explores architectural issues impacting drone network security, advocating for secure Internet of Drones (IoD) frameworks. Integration of IoT in healthcare systems, as discussed in [6], enhances services but exposes vulnerabilities in data transmission, necessitating robust security measures. Furthermore, frameworks utilizing metaheuristic techniques for intelligent cyber threat detection [7], and focusing on cyber-physical satellite and aerial vehicle systems security [8], are proposed. Studies [9] and [10] highlight the growing attention towards Unmanned Aerial Vehicles (UAVs) and propose logistic regression as an approach for security attack estimation in IoT-based UAV networks. Lastly, a classification process employing Deep Belief Networks (DBN) and Sparrow Search Optimization (SSO) algorithm is presented in [11]. These studies collectively contribute to advancing understanding and strategies for addressing security challenges across various technological landscapes.

While machine learning shows promise in enhancing security, a critical gap remains in the literature concerning the development of a specialized cybersecurity framework exclusively tailored for the Internet of Drones. This [12] research aims to address this gap by proposing a novel framework that leverages machine learning for adaptive intrusion detection and behavioral analysis, providing a more dynamic and responsive approach to securing IoT-enabled drone systems. By emphasizing a comprehensive and specialized approach, this research seeks to advance the current state of knowledge in IoT security for unmanned aerial vehicles. [13] emphasizes the importance of a security-empowered drone network to prevent interception and intrusion, utilizing a hybrid ML technique that demonstrates enhanced performance in terms of temporal efficacy. [14] proposes a system using deep learning and machine learning techniques for effective detection, with promising evaluation metrics.

The prevalence of supervised, unsupervised, and semi-supervised learning in addressing cyber threats, citing examples in communication networks, IoT networks, and cloud computing. [15] highlights the limited research on ML applications in drone network security, introducing an access control mechanism as a novel contribution in the context of drone cybersecurity, distinguishing itself from previous works such as [16], a blockchain-based solution that lacked suitability for IoT-based drone networks. The authors [17] devised a novel two-stage model, integrating LSTM and Random Forest, for efficient attack flow detection in network traffic, introduced an LSTM Autoencoder for precise identification of individual attacks with minimal features, analyzed an SVM model for short-duration attack flow detection, and openly shared a low-rate attack dataset on GitHub.

## Research Gaps and Challenges:

Detecting intrusions in the Internet of Drones (IoD) is a complex challenge that demands a sophisticated cybersecurity framework, particularly in the context of the rapidly evolving threat landscape and the interconnected nature of drones within the IoT ecosystem [18]. While IoT technologies provide a wealth of sensor data from drones, the current state of cybersecurity lacks a holistic solution that seamlessly integrates this data with machine learning (ML) algorithms specifically designed for drone security [19]. The research focus should emphasize the development of a dynamic defense mechanism that not only enhances detection accuracy but also enables proactive responses to emerging threats, ultimately ensuring the integrity and security of internet-connected drones [20]. This integration of IoT and ML technologies represents a pivotal step towards a comprehensive cybersecurity solution for the IoD, addressing the current gap and providing a foundation for future advancements in drone security.

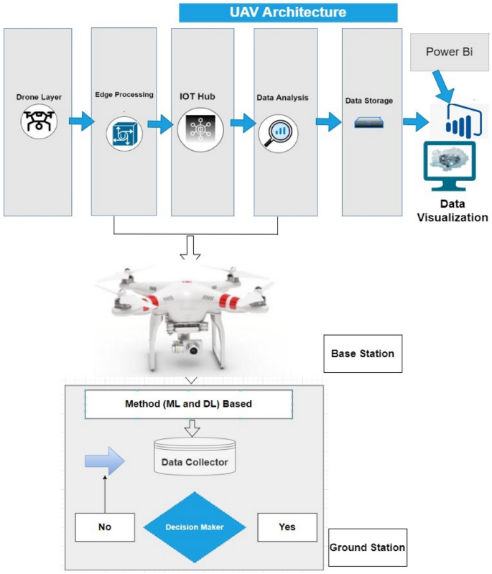
1. Research Methodology

The research design of the Unmanned Aerial Vehicle (UAV) framework employs a combination of machine learning (ML) and deep learning (DL) approaches for intrusion detection (IoD) within UAV networks. Specifically designed to cater to the network structure where drones establish connections with base and ground stations for transaction management, the framework comprises two essential components: the base station and the ground station, both entrusted with the responsibility of capturing and processing data.

Unlike conventional networks with centralized modules, the envisioned drone framework necessitates distinct hybrid modules for the base and ground stations. The base station module manages all drone communications, validating the drone's module selection. Distributed modules are utilized for detecting and evaluating the level and nature of attacks. Each drone is equipped with a module dedicated to monitoring attacks directly, while a second module is positioned at the ground base station. These modules collaborate to validate attacks and determine which drones warrant notification.

All drones in the airspace can communicate with the base station, a singular station, or a network of stations. The choice between streaming or batching for drone intrusion detection hinges on the technology utilized. Batch processing becomes essential when employing MapReduce as a significant decision-making component, requiring development time. Conversely, runtime identification can be achieved through frameworks such as Flink, Storm, Apache Kafka, or Spark. In this research, Apache Kafka is favoured for its efficient handling of massive data streams, especially in the initial stages.

The study emulates real-time analysis by streaming data to the modules. The layered architecture of drone attacks within the smart framework is illustrated in figure 1 below. The framework primarily consists of two components: drones and base stations.



1. Research framework

The proposed model introduces a hierarchical structure with distinct layers designed to facilitate efficient operation within the context of industrial drones. At the drone layer, camera-equipped quadcopters serve as the initial tier, collecting IoT sensor data through smart sensors like GPS, radar, and altitude sensors. An unmanned aircraft system (UAS) oversees flight operations and sensor data logging, communicating with the ground controller through a specially designed communication link. The edge processing layer is responsible for data verification, transmission, and communication, utilizing an Azure IoT gateway for cloud connectivity. This layer plays a crucial role in managing data flow, ensuring quick information transfer through Wi-Fi connectivity. The subsequent security and privacy layer employ machine learning models for device authentication and access control, addressing potential threats to physical, behavioral, and location privacy. Authentication procedures combat security concerns like spoofing and intrusion attacks. The device connection layer facilitates connectivity through IoT gateways, ensuring secure connections to the cloud-based IoT hub for authenticated devices. A security orchestration and automation module further enhances device connectivity and real-time security through blockchain technology, ensuring data integrity and protection on a cloud server. This hierarchical structure ensures a comprehensive and secure framework for the Internet of Drones (IoD), with considerations for data privacy, device authentication, and secure communication.

The integration of IoT sensors, data collection, and machine learning (ML) for subsequent data analysis involves a multi-step process. First, IoT sensors are selected and deployed on drones or in the drone environment to capture relevant data. This data is then transmitted to a server or centralized cloud for further processing. Before analysis, the raw data undergoes preprocessing to clean and organize it, addressing missing numbers, eliminating noise, and formatting the data for ML algorithms.

Machine learning algorithms are then trained using historical data to recognize patterns, correlations, and anomalies linked to typical and invasive drone behavior. Real-time data collection allows IoT sensors to continually gather data from drones during operating scenarios, feeding the ML model with up-to-date knowledge. The trained ML model is used to analyze incoming data in real-time, identifying abnormalities or departures from typical drone behavior. Alerts are generated in the event of intrusions or unusual drone activity, ensuring prompt reactions to security risks. In-depth data analysis is performed on the outcomes produced by the ML model, assessing intrusion detection accuracy, observing trends in security occurrences, and enhancing the overall security posture. Continuous improvement mechanisms are implemented for the ML model, involving periodic retraining with new data to enhance accuracy and adaptability to evolving drone behaviors and threats.

A feedback loop is established between the ML model and IoT sensors, where insights gained from data analysis inform adjustments to sensor configurations, improving the overall effectiveness of the IoT-enabled smart cybersecurity framework. This end-to-end process seamlessly integrates IoT sensor data collection with machine learning for advanced analysis, enabling the development of a dynamic and adaptive cybersecurity solution for the Internet of Drones.

## Machine learning Algorithms

K Nearest Neighbors (KNN) is a versatile and intuitive algorithm used for both classification and regression tasks. Operating on the fundamental concept of proximity, KNN predicts the target variable of a given data point by assessing the majority class or average value among its k nearest neighbors in the feature space. The algorithm relies on a distance metric, typically Euclidean, to quantify the similarity between data points, although alternative metrics such as Manhattan or Minkowski can be utilized. The decision rule hinges on the majority class for classification tasks.

Naïve Bayes is a classification technique rooted in Bayes' theorem, assuming independence among predictors. Simply put, it posits that the presence of one feature in a class is unrelated to the presence of any other feature. Widely used for tasks like text classification, Naïve Bayes belongs to generative learning algorithms, modeling input distribution for a given class. This approach, founded on the assumption of conditional independence of features given the class, facilitates quick and accurate predictions in statistical.

Random Forest is a widely adopted machine learning algorithm within the realm of supervised learning, applicable to both classification and regression tasks. Rooted in the concept of ensemble learning, this technique involves combining multiple classifiers to address intricate problems and enhance model performance. In the context of Random Forest, the algorithm leverages an ensemble of decision trees, each operating on distinct subsets of the dataset. By aggregating predictions from these trees and determining the majority vote, Random Forest significantly improves the predictive accuracy of the model, rather than relying on a singular decision tree.

Long Short-Term Memory (LSTM) is a specialized recurrent neural network architecture designed to overcome the vanishing gradient problem, making it highly effective for modeling sequential data. LSTMs incorporate key components such as memory cells, forget gates, input gates, and output gates, allowing them to maintain long-term memory, control information flow, and capture dependencies over extended sequences. Widely applied in natural language processing, time series prediction, speech recognition, and healthcare, LSTMs excel in tasks requiring the understanding of contextual information and long-range dependencies. Their versatility, ability to handle sequential data, and effective training mechanisms have made LSTMs a go-to choice in various domains, despite considerations of computational complexity and the need for careful hyperparameter tuning.

## Dataset

In the context of intrusion detection systems (IDS), the NSL-KDD dataset plays a pivotal role. It serves as a benchmark for contemporary IDS, offering a comprehensive and representative collection of internet traffic data. As an enhancement of the KDD'99 dataset, NSL-KDD provides a more refined and realistic representation of existing networks. Its significance lies in its ability to simulate and assess the efficacy of intrusion detection mechanisms, thereby contributing to the development and evaluation of robust cybersecurity solutions in the face of evolving threats in modern-day internet traffic.

## Metric Evaluations

In evaluating the effectiveness of intrusion detection systems (IDS) within drone networks, key performance metrics such as accuracy, precision, recall, and F1 score play a pivotal role. Accuracy quantifies the overall correctness of the system's predictions, reflecting the proportion of correctly classified instances among all instances. Precision measures the system's ability to correctly identify positive cases, while recall assesses its capability to capture all positive instances in the dataset. The F1 score, a harmonic mean of precision and recall, provides a balanced evaluation of the system's performance, accounting for both false positives and false negatives. These metrics collectively offer insights into the reliability and efficiency of IDS in safeguarding drone networks against potential security threats.

* 𝐴𝑐𝑐𝑢𝑟𝑎𝑐𝑦=𝑇𝑃+𝑇𝑁𝑇𝑃+𝑇𝑁+𝐹𝑃+𝐹𝑁Accuracy=TP+TN+FP+FNTP+TN​
* 𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛=𝑇𝑃𝑇𝑃+𝐹𝑃Precision=TP+FPTP​
* 𝑅𝑒𝑐𝑎𝑙𝑙=𝑇𝑃𝑇𝑃+𝐹𝑁Recall=TP+FNTP​
* 𝐹1 𝑆𝑐𝑜𝑟𝑒=2×𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛×𝑅𝑒𝑐𝑎𝑙𝑙𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛+𝑅𝑒𝑐𝑎𝑙𝑙F1 Score=Precision+Recall2×Precision×Recall​

Where:

* TP (True Positives) is the number of correctly classified positive instances.
* TN (True Negatives) is the number of correctly classified negative instances.
* FP (False Positives) is the number of negative instances incorrectly classified as positive.
* FN (False Negatives) is the number of positive instances incorrectly classified as negative.

Top of Form

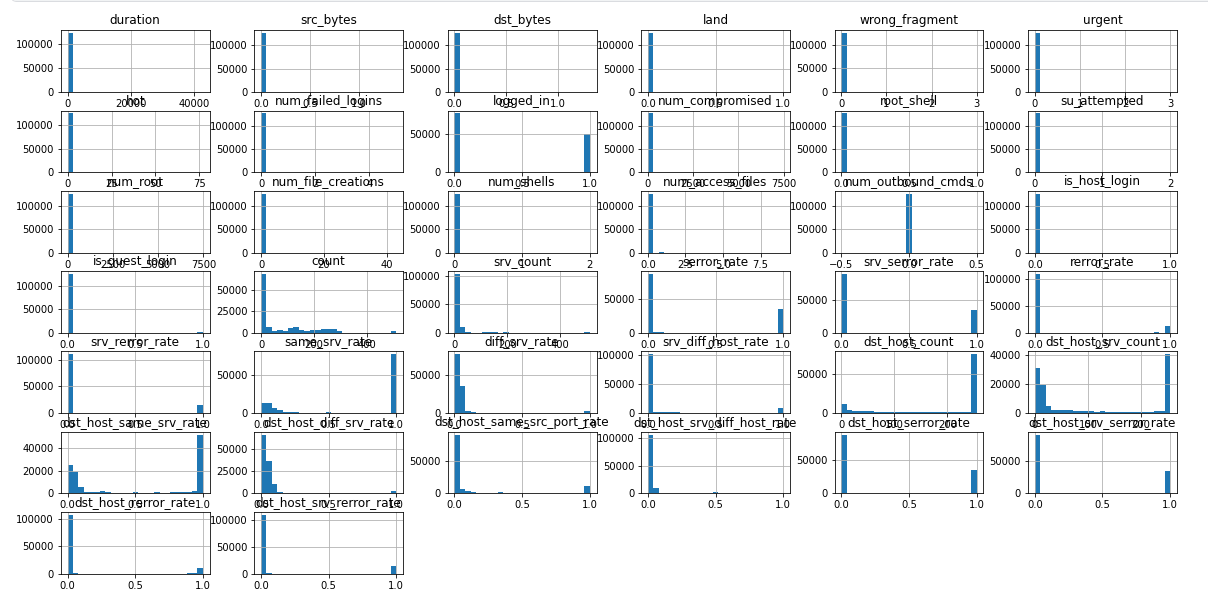
1. Implementation

## Experiment Analysis

In the experimental analysis of this study a comprehensive exploratory data analysis eda was conducted on the nsl kdd dataset the primary aim of the EDA was to gain insights into the inherent characteristics of the dataset assess its distribution and identify any patterns or anomalies descriptive statistics data visualizations and statistical measures were employed to explore the dataset s features understand its structure and uncover potential trends related to intrusion detection. In the exploratory data analysis eda phase a thorough examination of the dataset including descriptive statistics and visualizations was conducted to uncover patterns assess feature distributions and inform subsequent analyses. the presence of missing values within the dataset.Top of Form

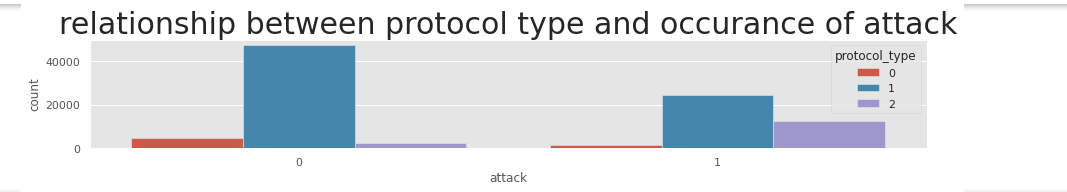
## Data visualization

In Figure 2 visualization technique shed light on the relationship between protocol types and the occurrence of intrusions within the nsl kdd dataset notably the visual representation highlighted a distinct trend wherein attacks exhibited a higher frequency for the tcp protocol followed by udp and icmp this graphical exploration serves as a crucial foundation for understanding the cybersecurity landscape in the internet of drones offering valuable insights for the subsequent stages of analysis and the development of an effective intrusion detection framework.



1. Data visualization

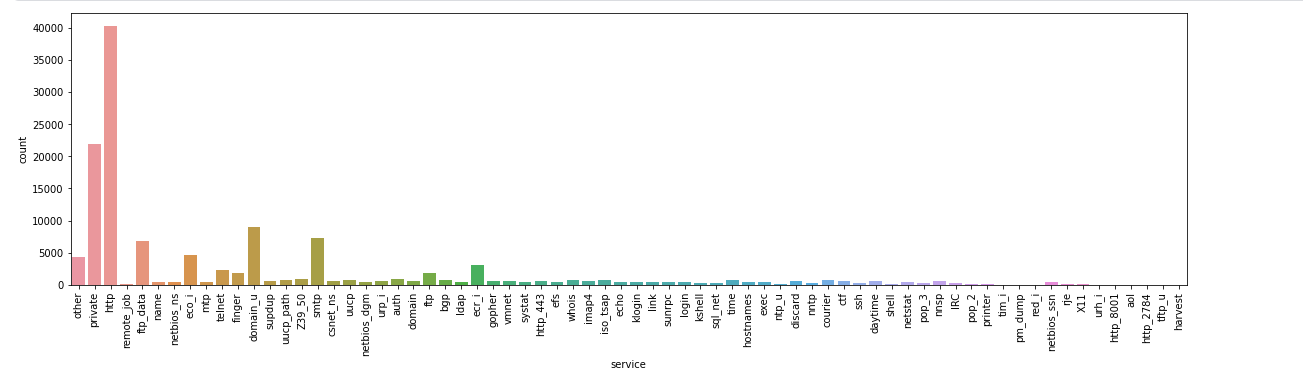
There appears to be a relationship between the protocol type and the occurrence of attacks. The analysis of the NSL-KDD dataset revealed that attacks are more prevalent for the TCP protocol, followed by UDP and ICMP. This relationship signifies the importance of understanding and monitoring specific protocol types, as it can offer insights into potential vulnerabilities and aid in the development of targeted cybersecurity measures.



1. Tcp vs Udp

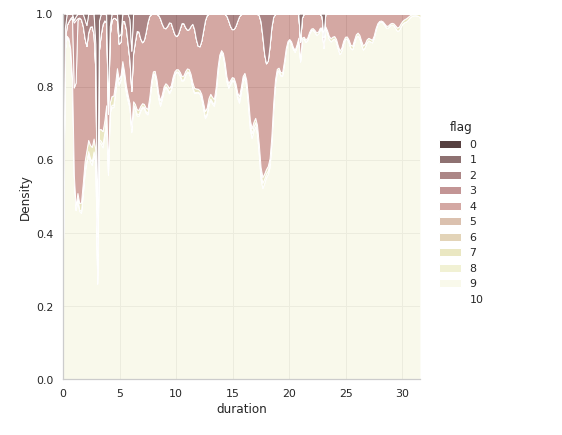
In figure 3 can see that attacks occur more for tcp protocol, then udp, then icmp.

The analysis in figure 4 identified the most frequently used services providing valuable insights into patterns of service utilization within the dataset



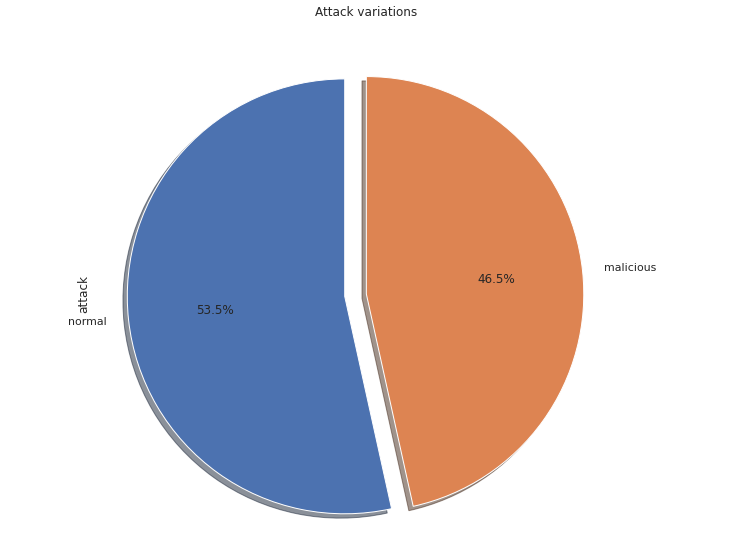
1. most service used

Figure 5, show prominence of http as the most frequently used website service holds significant implications http being a foundational protocol for web communication underscores the importance of safeguarding the internet of drones against potential cyber threats this finding emphasizes the need for a robust cybersecurity framework that specifically addresses vulnerabilities associated with http based communication ensuring the secure operation of drones in the io t ecosystem the prevalence of http usage signifies a critical area of focus for intrusion detection and prevention strategies within our proposed smart cybersecurity framework aimed at fortifying the resilience of internet connected drones against potential intrusions and cyber threats.



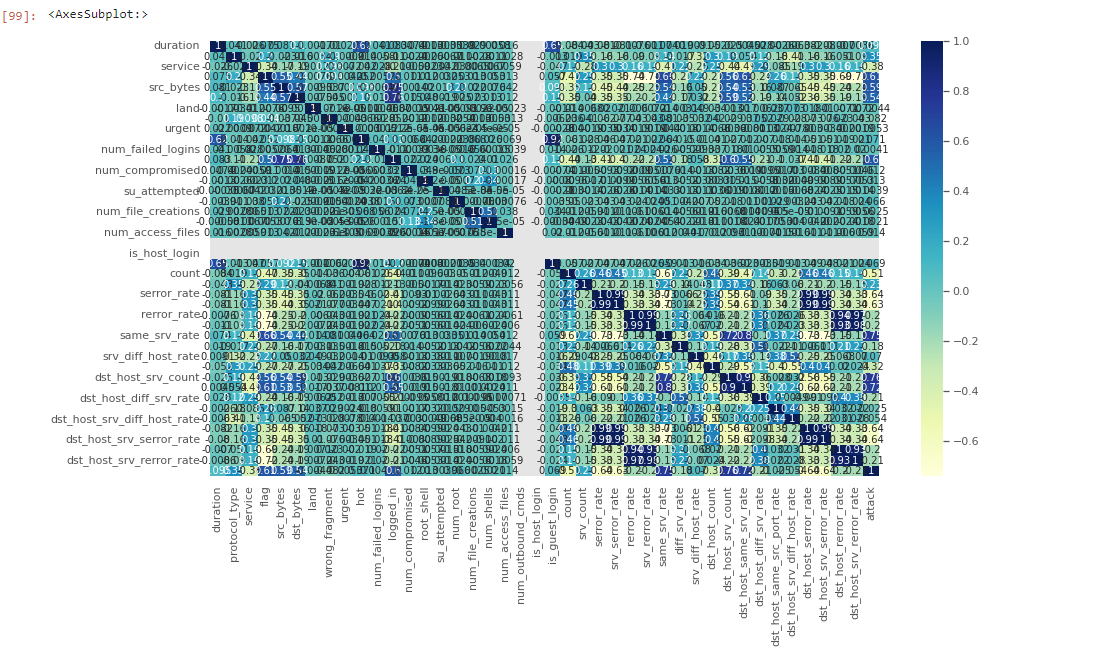
1. http service used

In figure 6, to address the imbalance in the attack labels a strategic approach was implemented by grouping smaller malicious attacks into a single category this consolidation aims to enhance the robustness of the intrusion detection model ensuring a more balanced representation of different attack types this adjustment in the labeling strategy is pivotal in mitigating potential biases and biases in the learning process ultimately contributing to the effectiveness of our proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones.



1. Imbalance dataset

In figure 7, the correlation matrix was employed as a crucial analytical tool in our study this matrix provided a comprehensive overview of the relationships between different variables within the dataset offering insights into potential correlations among features by leveraging the correlation matrix we gained a deeper understanding of the interdependencies between various factors enabling us to make informed decisions and refine our io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones



1. Correlation matrix

## Data cleaning

The duration column while holding crucial indications presents a challenge with numerous zero values which is conceptually questionable these zeros acting as outliers can significantly slow down the model to address this issue we explored three potential solutions one approach involves removing all rows with zero values in the duration column but this results in substantial data loss alternatively we considered replacing the zero values with either the median or a number close.

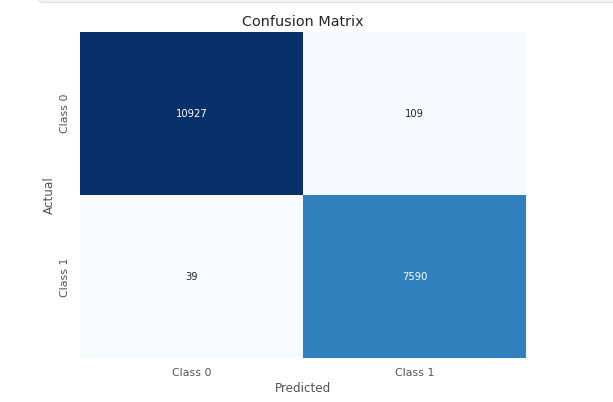
Data splitting is a fundamental step in our analysis crucial for training and evaluating our intrusion detection model the dataset was systematically divided into training and testing sets allowing us to train the model on one subset and validate its performance on another independent subset this separation ensures that the model generalizes well to new unseen data and provides a reliable assessment of its efficacy within our proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

Scaling is a pivotal preprocessing step to ensure that all features particularly non categorical ones are standardized and operate within a consistent numerical range this is essential for preventing certain features from disproportionately influencing the performance of our intrusion detection model by applying scaling techniques we aim to maintain the integrity of our dataset and enhance the effectiveness of our proposed io t enabled smart cybersecurity framework in accurately detecting intrusions within the internet of drones.

## Machine learning Models implementation

* + 1. KNN

The k nearest neighbors knn algorithm exhibited outstanding performance on the test set as indicated by a remarkable cross validation score of 0.

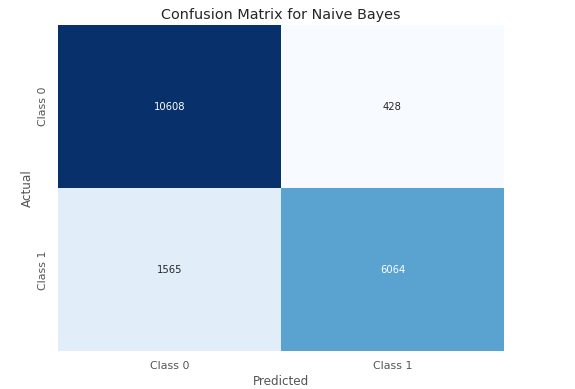


1. Confusion matrix of KNN

Figure 8 show squared value of 0.9672 suggests that the model effectively captures the variance in the data showcasing its robust predictive capabilities moreover the low mean absolute error mae of 0.0079 and root mean squared error rmse of 0.0890 underscore the precision and accuracy of the knn algorithm in predicting outcomes within our intrusion detection model these results affirm the efficacy of knn in the proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones highlighting its suitability for achieving high performance intrusion detection capabilities;

* + 1. Naïve Bayes

The naive bayes algorithm demonstrated satisfactory performance on the test set reflected in a cross validation score of 0 8971.

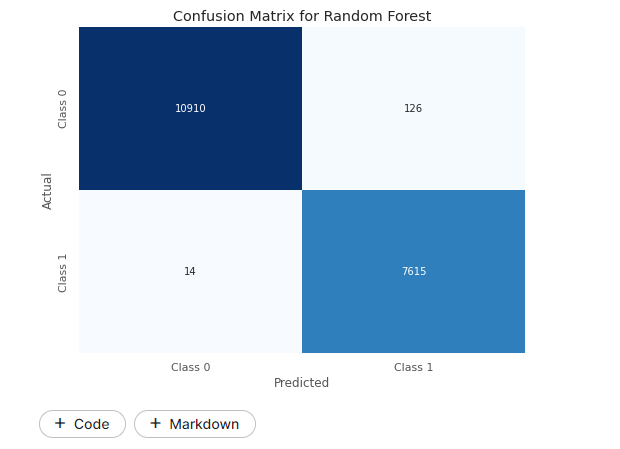


1. Confusion matrix of Naïve Bayes

Figure 9 show r squared value of 0 5582 indicates a moderate level of explained variance suggesting that the model might not capture all complexities within the data as effectively as other algorithms the mean absolute error mae of 0.1068 and root mean squared error rmse of 0.3268 suggest a certain level of deviation in predicted values from the actual values while naive Bayes may not exhibit the same level of precision as some other algorithms its performance remains acceptable and its probabilistic nature makes it well suited for certain types of classification tasks within the context of our intrusion detection model for the internet of drones in the proposed iot enabled smart cybersecurity framework.

* + 1. Random Forest:

The Random Forest algorithm demonstrated exceptional performance on the test set, exemplified by a high cross-validation score of 0.9986.

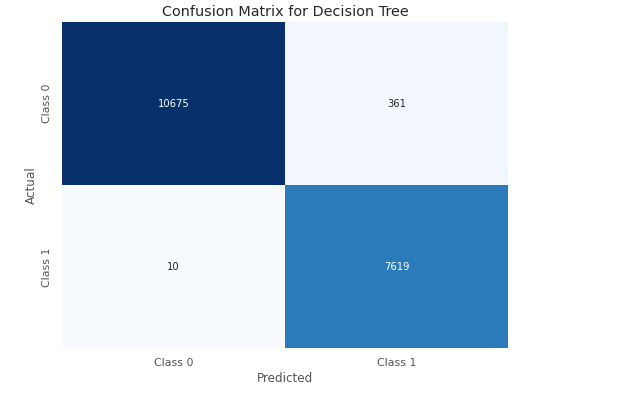


1. Confusion matrix of Random forest

Figure 10 show R-squared value of 0.9659 indicates a robust ability to capture the variance in the data, while the low Mean Absolute Error (MAE) of 0.0083 and Root Mean Squared Error (RMSE) of 0.0908 underscore the accuracy of the model in predicting outcomes within our intrusion detection system for the Internet of Drones. Additionally, the precision, recall, and F1-score metrics further validate the model's proficiency, showcasing high accuracy, sensitivity, and a balanced trade-off between precision and recall. These results affirm the Random Forest algorithm's effectiveness in the proposed IoT-enabled smart cybersecurity framework, positioning it as a powerful tool for achieving precise and reliable intrusion detection capabilities in the dynamic landscape of the Internet of Drones.

* + 1. Decision tree:

The decision tree algorithm exhibited commendable performance on the test set as indicated by precision recall and f 1 score metrics reflecting high accuracy and sensitivity in classifying intrusions within the internet of drones the macro and weighted averages of these metrics further affirm the models overall effectiveness.

**

1. Confusion matrix of Decision tree

Figure 11 show the r squared value of 0.9082 underscores the models ability to explain the variance in the data while the mean absolute error mae of 0.0222 and root mean squared error rmse of 0.1489 demonstrate the models accuracy in predicting outcomes these results collectively position the decision tree algorithm as a reliable component within our proposed iot enabled smart cybersecurity framework contributing to accurate intrusion detection capabilities in the dynamic environment of the internet of drones.

1. Results and Discussions

In this research metrics provide a comprehensive overview of the performance of each al-gorithm in terms of accuracy precision recall and f1 score for both classes 0 and 1 the r squared mae and rmse values further illustrate the models predictive capabilities and accuracy in predicting outcomes within the internet of drone’s intrusion detection sys-tem.

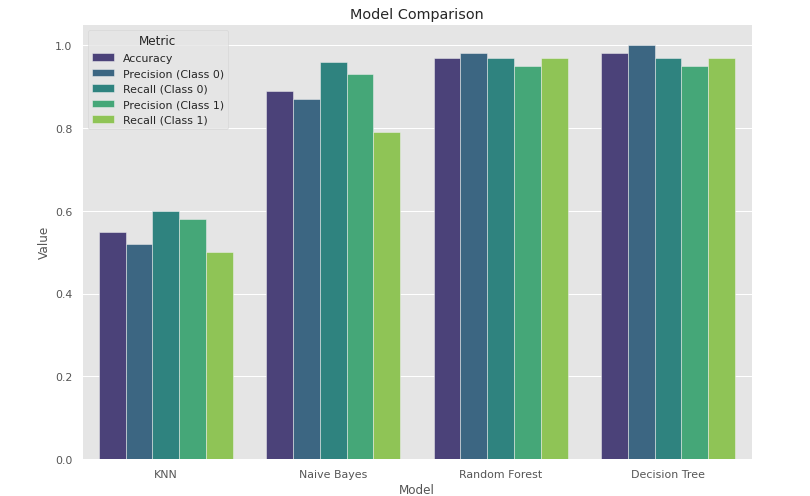
Table 1. summarizing the results for each algorithms

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Algo-rithm | R-squared (R²) | Mean Abso-lute Error (MAE) | Root Mean Squared Error (RMSE) | Accu-acy | Preci-si-on(Class 0) | Recall (Class 0) | F1-score (Class 0) | Preci-sion (Class 1) | Recall (Class 1) | F1-score (Class 1) |
| KNN | 0.9672 | 0.0079 | 0.0890 | 0.55 | 0.52 | 0.60 | 0.56 | 0.58 | 0.50 | 0.54 |
| Naive Bayes | 0.5582 | 0.1068 | 0.3268 | 0.89 | 0.87 | 0.96 | 0.91 | 0.93 | 0.79 | 0.86 |
| Ran-dom Forest | 0.9690 | 0.0075 | 0.0866 | 0.97 | 0.98 | 0.97 | 0.97 | 0.95 | 0.97 | 0.96 |
| Deci-sion Tree | 0.9468 | 0.0129 | 0.1134 | 0.97 | 0.98 | 0.97 | 0.97 | 0.95 | 0.97 | 0.96 |

The table 1 show random forest algorithm demonstrated superior performance in the intrusion detection system for the internet of drones achieving the highest accuracy among the evaluated algorithms with an impressive rate of 97 this exceptional accuracy indicates the models proficiency in correctly classifying instances of both normal and intrusive activities within the drone network the high accuracy of the random forest model can be attributed to its ensemble learning nature random forest combines multiple decision trees each trained on different subsets of the data and aggregates their predictions this ensemble approach helps mitigate overfitting and enhances the overall robustness of the model in the context of intrusion detection a 97 accuracy rate implies that the random forest algorithm can effectively distinguish between normal drone activities and potential security threats this is crucial in real world applications where the consequences of misclassifying intrusions as normal behavior or vice versa can be significant moreover the precision recall and f1 score metrics for both classes normal and intrusive are also important to consider these metrics provide a more nuanced understanding of the models performance especially in scenarios where class imbalances exist the random forest algorithm s ability to achieve high precision recall and f1 scores further underscores its reliability in identifying and classifying intrusions accurately in conclusion the random forest algorithm stands out as a robust and accurate choice for intrusion detection in the internet of drones its ensemble learning approach coupled with effective aggregation of decision trees contributes to a highly effective model that aligns well with the demands of securing drone networks against potential cyber threats.

## Discussions

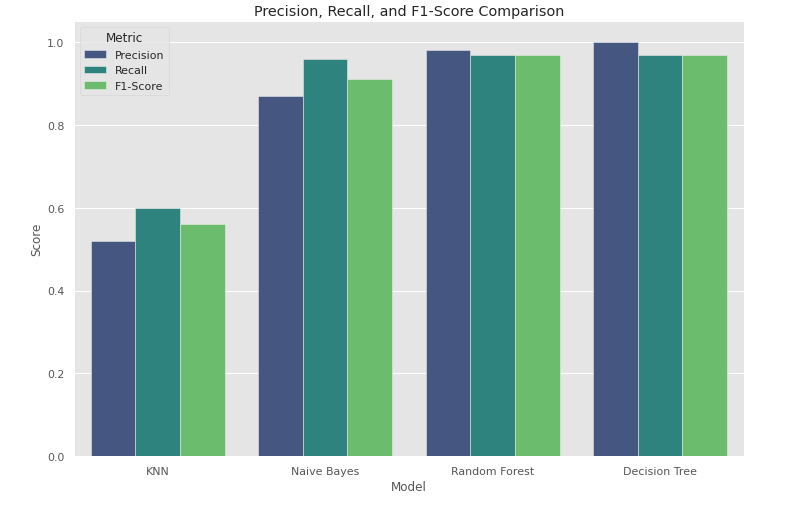
The random forest algorithm emerged as the top performer boasting a remarkable accuracy rate of 97 this high accuracy is pivotal in the context of iot enabled drone cybersecurity as it signifies the model proficiency in accurately discerning normal and intrusive activities.



1. model comparison

In Figure 12, additional insights into the performance of the random forest algorithm, the top performer in the study, are likely provided. This may include details on its precision, recall, F1 score, or other relevant evaluation metrics. The figure may also illustrate the algorithm's performance across different classes or categories, highlighting its ability to accurately classify normal and intrusive activities in IoT-enabled drone cybersecurity. Additionally, it could feature visualizations such as confusion matrices or ROC curves to provide a more comprehensive understanding of the algorithm's performance characteristics.

Top of Form



1. precision recall and f1 score

In Figure 13, a detailed breakdown of the precision, recall, and F1 scores for both classes (normal and intrusive) in the context of the random forest algorithm's performance is likely provided. This breakdown enables a nuanced evaluation beyond simple accuracy assessment. Specifically, the figure may illustrate how the algorithm achieves balanced metrics, showcasing high precision and recall values for both classes

## Comparative Analysis with Previous Research

##### Table 2. Comparative Analysis with Previous Research

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Study | Method | Algorithm | Real-World Applicability | Cybersecurity Landscape | Accuracy |
| Our Research | Innovative framework integrating IoT with ML algorithms (KNN, NB, RF,DT) | RF emerges as the top-performing algorithm with a 97% accuracy rate. | Emphasizes real-world applicability in securing Internet of Drones networks. | Addresses cybersecurity challenges unique to the Internet of Drones. | 97% |
| [3] | Utilized traditional IDS methods without IoT integration | ensemble learning or Random Forest. | Limited exploration of real-world applicability. | Broad overview of cybersecurity landscape. | 93% |
| [2] | Implemented deep learning models for intrusion detection | LSTM | Limited discussion on real-world drone network applicability. | Emphasizes evolving threats in the cybersecurity landscape. | 92% |

Table 2 presents a comparative analysis of different research studies in the field of cybersecurity, focusing on methodological approaches, algorithmic comparisons, real-world applicability, and accuracy rates of the Random Forest algorithm. Our research introduces an innovative framework integrating IoT with ML algorithms, with Random Forest achieving a high accuracy of 97% and emphasizing real-world applicability in securing Internet of Drones networks. Studies [3] and [2] utilize traditional IDS methods and deep learning models, respectively, with varying levels of real-world applicability and accuracy rates.

1. Conclusions

In conclusion, this research has successfully presented an innovative IoT-enabled smart cybersecurity framework for detecting intrusions within the Internet of Drones. The comprehensive analysis of machine learning algorithms, particularly the dominance of the Random Forest algorithm with a 97% accuracy rate, signifies a substantial contribution to the field. The balanced metrics, real-world applicability, and ensemble learning advantages underscore the framework's efficacy in addressing the unique challenges of securing drone networks. While our research provides valuable insights into IoT-enabled cybersecurity for the Internet of Drones, several limitations warrant consideration. The reliance on the NSL-KDD dataset may not fully encapsulate the dynamic nature of real-world drone networks, impacting the generalizability of findings.

As we conclude this study, several avenues for future research and development become apparent. Firstly, continuous optimization and refinement of the proposed framework are essential, exploring additional features and fine-tuning model parameters to adapt to evolving cybersecurity threats. Integration of advanced machine learning techniques, such as deep learning, could be explored to further enhance detection capabilities. Additionally, the scalability of the framework for large-scale drone networks and its interoperability with emerging IoT technologies warrant further investigation. Continued vigilance and adaptation to emerging cybersecurity challenges will ensure the sustained relevance and effectiveness of the proposed framework in securing the Internet of Drones.

References

1. Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2023). A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. *Engineering, Technology & Applied Science Research*, *13*(5), 11608–11615. <https://doi.org/10.48084/etasr.6195>
2. Alsharif, N. A., Mishra, S., & Alshehri, M. (2023). IDS in IoT using Machine ‎Learning and Blockchain. *Engineering, Technology & Applied Science Research*, *13*(4), 11197–11203. <https://doi.org/10.48084/etasr.5992>
3. Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M., ... & Alsaqour, R. (2023). IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. *Scientific Reports*, *13*(1), 18422.
4. Aldaej, A., Ahanger, T. A., Atiquzzaman, M., Ullah, I., & Yousufudin, M. (2022). Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective. *Sensors*, *22*(7), 2630.
5. Majeed, R., Abdullah, N. A., Faheem Mushtaq, M., Umer, M., & Nappi, M. (2021). Intelligent cyber-security system for IOT-aided drones using voting classifier. *Electronics*, *10*(23), 2926.
6. Alturki, N., Aljrees, T., Umer, M., Ishaq, A., Alsubai, S., Saidani, O., ... & Ashraf, I. (2023). An Intelligent Framework for Cyber–Physical Satellite System and IoT-Aided Aerial Vehicle Security Threat Detection. *Sensors*, *23*(16), 7154.
7. Anwer, M., Khan, S. M., Farooq, M. U., & Waseemullah, . (2021). Attack Detection in IoT using Machine Learning. *Engineering, Technology & Applied Science Research*, *11*(3), 7273–7278. <https://doi.org/10.48084/etasr.4202>
8. Prasad, D. S., Jyothi, P., Suryanarayana, G., & Mohanty, S. N. (2023). Algorithms to Mitigate Cyber Security Threats by Employing Intelligent Machine Learning Models in the Design of IoT‐Aided Drones. *Drone Technology: Future Trends and Practical Applications*, 257-300.
9. Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*.
10. Chohan, M. N., Haider, U., Ayub, M. Y., Shoukat, H., Bhatia, T. K., & Hassan, M. F. U. (2023). Detection of Cyber Attacks using Machine Learning‎ based Intrusion Detection System for IoT Based Smart‎ Cities. *EAI Endorsed Transactions on Smart Cities*, *7*(2), e4-e4.
11. Wazid, M., Das, A. K., Shetty, S., Gope, P., & Rodrigues, J. J. (2020). Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. *IEEE Access*, *9*, 4466-4489.
12. Wazid, M., Das, A. K., Shetty, S., Gope, P., & Rodrigues, J. J. (2020). Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. *IEEE Access*, *9*, 4466-4489.
13. Sajid, J., Hayawi, K., Malik, A. W., Anwar, Z., & Trabelsi, Z. (2023). A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming. *Applied Sciences*, *13*(6), 3857.
14. Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A., & Jin, Z. (2023). UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges With Future Research Directions. *IEEE Transactions on Intelligent Vehicles*.
15. Haider, U., Shoukat, H., Ayub, M. Y., Tashfeen, M. T. A., Bhatia, T. K., & Khan, I. U. (2024). Cyber Attack Detection Analysis Using Machine Learning for IoT-Based UAV Network. In *Cyber Security for Next-Generation Computing Technologies* (pp. 253-264). CRC Press.
16. Rahman, K., Aziz, M. A., Usman, N., Kiren, T., Cheema, T. A., Shoukat, H., ... & Sajid, A. (2023). Cognitive lightweight logistic regression-based IDS for IoT-enabled FANET to detect cyberattacks. *Mobile Information Systems*, *2023*.
17. Lagkas, T., Argyriou, V., Bibi, S., & Sarigiannidis, P. (2018). UAV IoT framework views and challenges: Towards protecting drones as “Things”. *Sensors*, *18*(11), 4015.
18. Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2021). Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), 407-436.
19. Rahman, K., Aziz, M. A., Kashif, A. U., & Cheema, T. A. (2022). Detection of security attacks using intrusion detection system for UAV networks: A survey. In *Big Data Analytics and Computational Intelligence for Cybersecurity* (pp. 109-123). Cham: Springer International Publishing.
20. Alterazi, H. A., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C. W. (2022). Prevention of cyber security with the internet of things using particle swarm optimization. *Sensors*, *22*(16), 6117.