iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73817

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

Analyzing Suspicious Behaviour in Automatic Tracking of Aircraft Data Using Machine Learning and Deep Learning

Rizwana Begum[1], Dr. M. Dhanalakshmi[2]
[1]*Post Graduate Student, MCA, Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India*
[2]*Professor, Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India*

Abstract: Ensuring the security and reliability of the Automatic Dependent Surveillance–Broadcast (ADS-B) system is essential for modern aviation safety. This research enhances its resilience by drawing on recent advancements in machine learning as well as deep learning, resulting in a robust detection mechanism. The system processes aircraft transmission data to identify deviations in ADS-B parameters and classify them into three categories: normal, potential anomaly, and confirmed anomaly. This classification enables early identification of irregular patterns that may indicate potential threats or abnormal operational behaviour, helping to mitigate faults or disruptions before they escalate. By employing advanced detection algorithms, the proposed approach strengthens ADS-B system security, supporting safer and more dependable air traffic operations.

Keywords: Automatic Dependent Surveillance–Broadcast (ADS-B), Aviation Security, Anomaly Detection, Machine Learning, Deep Learning, Aircraft Transmission Data, Air Traffic Safety

I. INTRODUCTION

Security of essential infrastructure, particularly avionics, has been a focus since 2003 because to its national security implications. Through programs like SESAR and NextGen, avionics systems—which were once closed and secure—are now being updated for efficiency. Automation has increased efficiency, but it has also created new cybersecurity problems and ambiguous security roles. Air traffic control uses ADS-B, which has been required since January 2020 under NextGen, to transmit flight data in real time. Even though there haven't been any significant breaches, the FAA is aware of threats including man-in-the middle assaults and eavesdropping. Due to their reliance on GPS and ADS-B, UAVs—which are being utilized more and more for missions that are more economical—are susceptible to jamming and spoofing. Although there are several ADS-B security solutions available, they frequently necessitate expensive infrastructure modifications or interfere with real-time operations, depriving contemporary systems of integrated security. Machine learning and deep learning-based irregularity detection methods offer effective alternatives that overcome these limitations.

A. Objective

The primary objective of this research is to improve the security and reliability of the Automatic Dependent Surveillance–Broadcast (ADS-B) system by applying machine learning and deep learning methods for anomaly detection. The goal is to:

1) Collect and preprocess ADS-B transmission data for accurate analysis.
2) Identify deviations and irregularities in flight parameters.
3) Develop models to classify data into normal, potential anomaly, and confirmed anomaly categories.
4) Strengthen ADS-B system security and support safer air traffic management.

This research aims to contribute toward building a more resilient and dependable ADS-B-based surveillance system, thereby enhancing the overall safety of aviation operations.

II. LITERATURE SURVEY

Martin Strohmeier et al. [1] conducted an in-depth study on the security of the ADS-B protocol, analysing various attack vectors in terms of their characteristics, frequency, and potential consequences. Their work also reviewed multiple countermeasures and introduced a structured framework that can serve as a reference point for subsequent research on ADS-B security. While the study provides a strong theoretical foundation, it remains largely conceptual and does not directly address practical anomaly detection techniques or real-time implementation.

Zhi-Jun Wu et al. [2] surveyed ADS-B security issues, classifying vulnerabilities by attack intent and security requirements. They reviewed countermeasures such as PKI and Spread Spectrum, and recommended a multi-layered security framework. However, the study remains conceptual and lacks experimental validation.

Edan Habler and Asaf Shabtai [3] proposed an anomaly detection method using an LSTM encoder–decoder model to identify irregular ADS-B messages. Their approach demonstrated effectiveness with a false alarm rate of 4.3% across six flight route datasets, showing the feasibility of deep learning for anomaly detection in aviation systems. However, the model exhibited performance variations across different routes, and the persistence of false alarms indicates challenges in achieving reliable deployment.

Zixi Liu et al. [4] explored the use of convolutional neural networks (CNN) for detecting Global Navigation Satellite System (GNSS) interference events within ADS-B data. Their approach confirmed the potential of deep learning in strengthening ADS-B security. Nonetheless, the work focused exclusively on GNSS interference, leaving other classes of ADS-B anomalies unaddressed, which restricts the generalizability of the approach.

III.METHODOLOGY OF PROPOSED SYSTEM

A. Proposed System

This proposed system employs machine learning and deep learning techniques to detect anomalies in ADS-B flight data. Deep learning models, such as Convolutional Neural Networks (CNNs) and Multi-Layer Perceptron's (MLPs), are used to capture complex and non-linear relationships, while traditional machine learning approaches, including Logistic Regression and AdaBoost, are trained to identify unusual patterns within ADS-B data. The system analyses ADS-B flight data to detect irregularities in air traffic, with MLPs particularly enhancing the detection of subtle and uncommon abnormalities. By integrating both machine learning and deep learning methods, the hybrid model improves overall performance and ensures more reliable anomaly detection.

B. Dataset Description

The dataset utilized in this study comprises records of aircraft movements collected via Automatic Dependent Surveillance–Broadcast (ADS-B) systems. Each record contains both standard operational parameters and instances of anomalous or irregular behavior. The primary objective of this dataset is to support the development of anomaly detection models using machine learning and deep learning techniques. The target variable is Anomaly_Label, which indicates whether a given record corresponds to normal operation or an anomaly.

The dataset spans multiple dimensions:

1) Aircraft Identification & Flight Details: Attributes such as Aircraft_ID, Transponder_Code, Squawk_Code, and Flight_Plan_Filed provide identification and planned operational details of the aircraft, enabling traceability and comparison against expected flight behaviour.

2) Positional Information: Fields including Latitude_Decimal and Longitude_Decimal capture the real-time geographical coordinates of the aircraft, supporting analysis of deviations from intended flight paths.

3) Altitude & Flight Level Metrics: Variables such as Altitude_ft and Flight_Level record the aircraft's current altitude and designated cruising level, which are critical for detecting unusual altitude fluctuations or deviations from assigned airspace levels.

4) Speed, Direction & Vertical Motion: Features including Speed_knots, Heading_Degrees, and Vertical_Speed_ft_min describe the aircraft's horizontal velocity, directional heading, and vertical motion. Abnormal variations in these values may indicate performance issues, safety risks, or non-compliance with flight plans.

5) Emergency & Safety Indicators: Attributes like Emergency_Code and Squawk_Code indicate critical operational states. While Squawk_Code represents the transponder code assigned by air traffic control, Emergency_Code signals emergency conditions.

6) Target Label: The Anomaly_Label attribute categorizes each record as normal, potential anomaly, or confirmed anomaly, providing the reference needed to evaluate and train anomaly detection models.

By combining structured preprocessing with aviation domain knowledge, this dataset enables the development of accurate and generalizable anomaly detection systems. Such models can identify irregular operational behaviours, safety risks, or malicious interference, supporting more reliable and resilient air traffic surveillance.

C. *System Architecture*

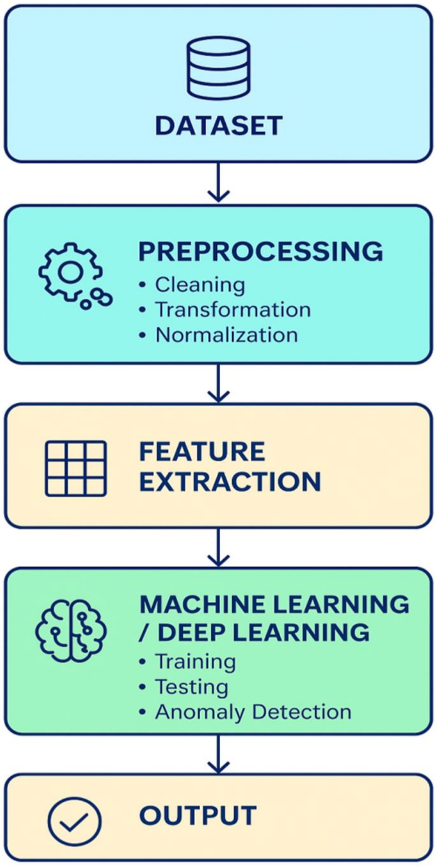


Figure-1: System Architecture

The proposed system adopts a modular and layered architecture to streamline data flow and enhance anomaly detection performance. Each stage in the pipeline contributes to building a reliable, interpretable, and scalable machine learning system.

D. *Methodology*

The proposed system is designed using a modular and layered architecture to streamline data processing and enhance anomaly detection performance on ADS-B flight surveillance data. The methodology involves five key stages, each contributing to building a robust and interpretable machine learning pipeline. The workflow is outlined as follows:

1) Data Collection

The process begins with collecting raw ADS-B surveillance data from various sources. This includes structured data such as aircraft identifiers, positional coordinates, speed, and altitude. Ensuring accurate and consistent data ingestion is essential for maintaining the reliability of downstream anomaly detection processes.

2) Data Preprocessing

Once collected, raw data undergoes extensive preprocessing to ensure quality and uniformity. This includes:

- Data Cleaning: Handling missing values, correcting inconsistencies, and removing noise.
- Data Transformation: Encoding categorical variables, scaling numerical features, and aggregating relevant fields.
- Data Normalization: Standardizing data distributions to ensure comparability across features.

These preprocessing steps ensure the dataset is optimized for feature extraction and model training.

3) Feature Extraction

At this stage, the system identifies and extracts meaningful features from the pre-processed data. Feature extraction reduces dimensionality, highlights key patterns, and enhances the learning capability of machine and deep learning algorithms. Both domain-specific features and automatically derived statistical indicators are considered**.**

4) Machine Learning and Deep Learning Layer

This core layer involves training and evaluating multiple machine learning and deep learning models to identify anomalies in flight data:

- Algorithms Used: AdaBoost Classifier, Logistic Regression, Convolutional Neural Network (CNN), and Multi-Layer Perceptron (MLP).
- Training and Validation: Models are trained using labelled flight data and validated to ensure generalization.
- Testing: Independent test sets evaluate model robustness.

5) Output and Decision Layer

The system provides actionable outputs based on the model predictions and anomaly scores. Results are classified into:

- Normal
- Potential Anomaly
- Confirmed Anomaly

IV. EXPERIMENTAL ANALYSIS AND RESULTS

A. Key Features

1) Integrated Machine Learning Pipeline
2) Advanced Anomaly Detection
3) Feature Engineering and Selection
4) ADS-B Security Enhancement
5) Multi-Model Comparison
6) Scalable Design
7) Feature-Rich Input Analysis
8) Interactive Web-Based Interface

B. Results

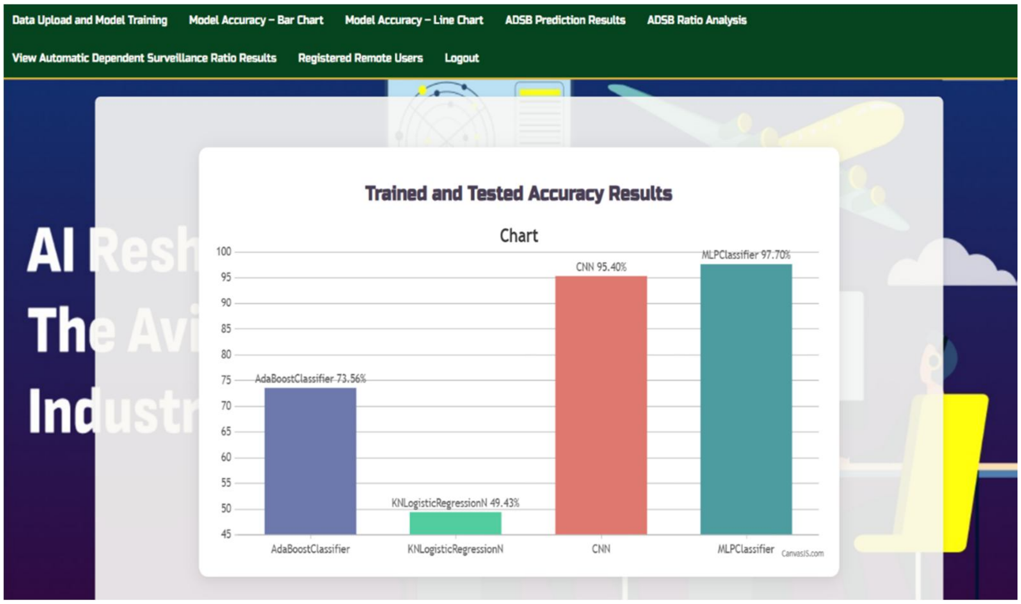
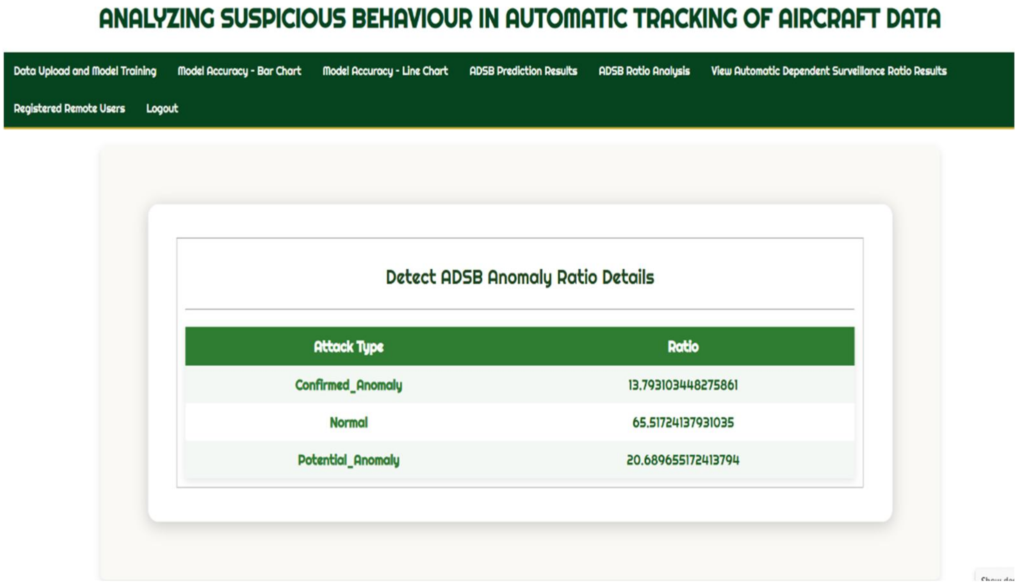


Figure-1: Accuracy Comparison of Machine Learning Model

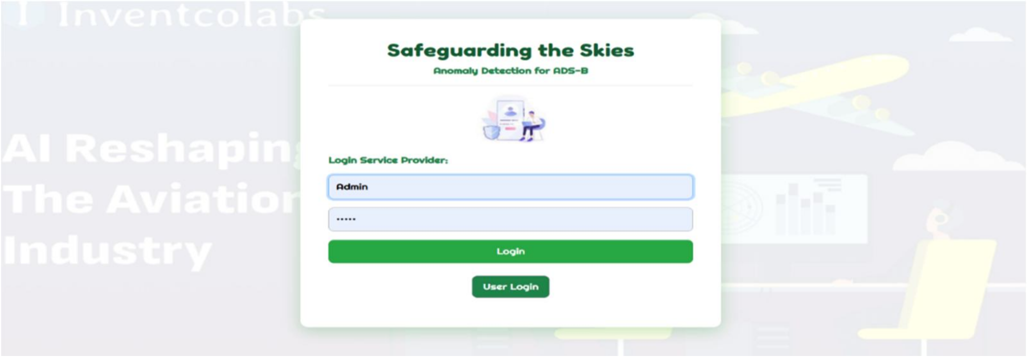


ANALYZING SUSPICIOUS BEHAVIOUR IN AUTOMATIC TRACKING OF AIRCRAFT DATA
Data Upload and Model Training
Model Accuracy - Bar Chart
Model Accuracy - Line Chart
ADSB Prediction Results
ADSB Ratio Analysis
View Automatic Dependent Surveillance Ratio Results
Registered Remote Users
Logout

Detect ADSB Anomaly Ratio Details

Attack Type	Ratio
Confirmed_Anomaly	13.793103448275861
Normal	65.51724137931035
Potential_Anomaly	20.689655172413794

Figure-2: Anomaly Ratio for Each Category

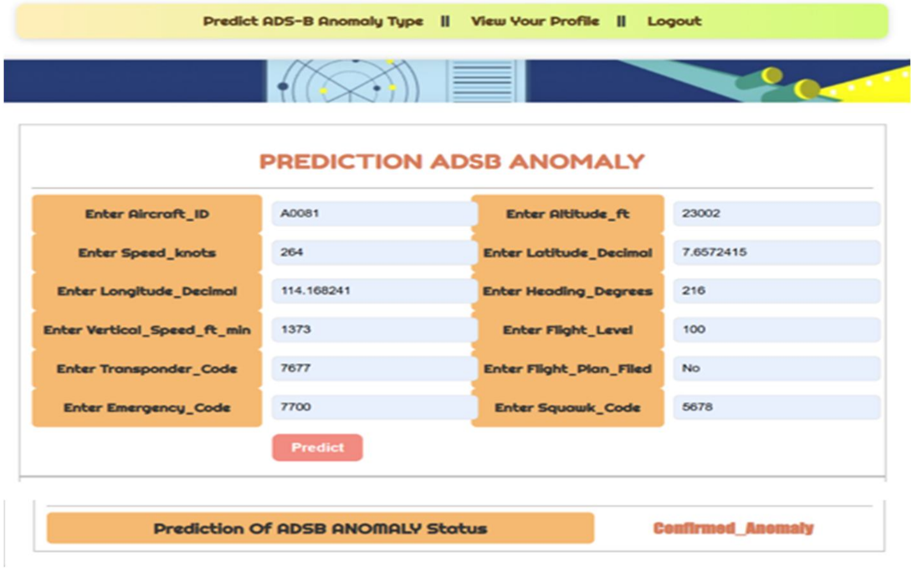


Login Service Provider:

Admin

·····

Figure-3: Admin Login Page



Enter Aircraft_ID	A0081	Enter Altitude_ft	23002
Enter Speed_knots	264	Enter Latitude_Decimal	7.6572415
Enter Longitude_Decimal	114.168241	Enter Heading_Degrees	216
Enter Vertical_Speed_ft_min	1373	Enter Flight_Level	100
Enter Transponder_Code	7677	Enter Flight_Plan_Filed	No
Enter Emergency_Code	7700	Enter Squawk_Code	5678

Prediction Of ADSB ANOMALY Status: Confirmed_Anomaly

Figure-5: Prediction Results Page

V. LIMITATIONS AND FUTURE SCOPE

While the proposed ADS-B anomaly detection system demonstrates effective classification using multiple machine learning and deep learning models, it has certain limitations. These include limited dataset diversity, challenges in obtaining accurately labelled anomalies, lack of real-time deployment, and reliance solely on ADS-B data without incorporating external contextual inputs like weather or flight plans. Additionally, model interpretability remains limited, and the absence of continuous learning restricts adaptability. Future work can explore advanced models such as transformers for improved accuracy, while multimodal data integration (e.g., ADS-B signals, flight plans, and weather) may enhance reliability. Continuous learning and reinforcement learning could enable adaptability to new scenarios, and Explainable AI (XAI) will improve transparency for stakeholders. Additionally, integrating real-time anomaly alerts with air traffic management systems can strengthen aviation safety. Expanding datasets across regions and routes will further improve generalization and robustness.

VI. CONCLUSION

This project makes use of a comprehensive dataset of aircraft flight data, which is necessary for creating and assessing sophisticated anomaly detection algorithms. It makes use of deep learning and machine learning methods to identify risky or irregular flight behaviours in real time, which could jeopardize aviation safety. Altitude, speed, heading, and emergency codes are among the key features that are analysed to promote proactive air traffic control and improved operational safety. The intricate structure of the dataset makes it easier to train models effectively, increasing predicted accuracy and allowing for automated surveillance. By improving anomaly detection capabilities, our research ultimately contributes to safer skies by improving the dependability of ADS-B systems and enabling intelligent, automated monitoring.

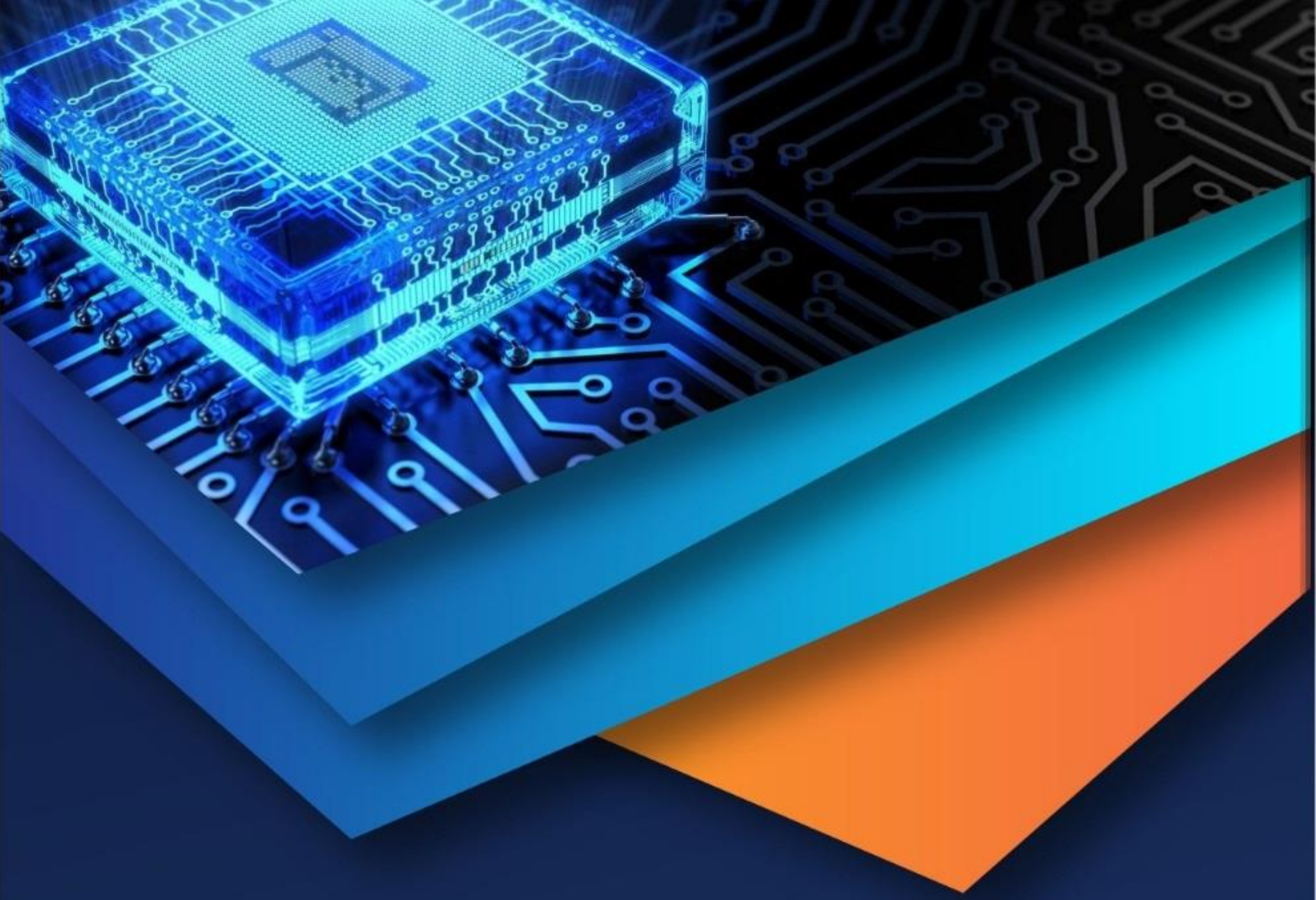
REFERENCES

[1] M. Strohmeier, V. Lenders, and I. Martinovic, “On the Security of the Automatic Dependent Surveillance–Broadcast Protocol,” IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066–1087, 2015. DOI:

[2] C. Habler and Y. Shabtai, “Using LSTM Encoder-Decoder Algorithm for Detecting Anomalous ADS-B Messages,” Computers & Security, vol. 78, pp. 155–173, Sept. 2018, DOI: https://doi.org/10.1016/j.cose.2018.07.004

[3] M. Riahi Manesh and N. Kaabouch, “Analysis of Vulnerabilities, Attacks, Countermeasures and Overall Risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) System,” International Journal of Critical Infrastructure Protection, vol. 19, pp. 16–31, Dec. 2017, DOI: https://doi.org/10.1016/j.ijcip.2017.10.002

[4] M. Pirolley, R. Couturier, M. Salomon, and F. Ambert, “[Poster] ADS-B anomaly detection in the surveillance of low-altitude aircrafts,” Journal of Open Aviation Science, vol. 1, no. 2, 2023. DOI: https://doi.org/10.59490/joas.2023.7200



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY