DRONE INTRUSION DETECTION USING DEEP LEARNING

B Sai Abhishek, Balam Ruchith Balaji, Chillakuru Hari
Department of Computer Science and Engineering, Amrita School of Computing,
Bengaluru, Amrita Vishwa Vidyapeetham, India.
BL.EN.U4AIE21015@bl.students.amrita.edu, BL.EN.U4AIE21017@bl.students.amrita.edu,
BL.EN.U4AIE21038@bl.students.amrita.edu

Abstract: This study aims to develop a method that utilizes complex computational systems to detect drone intrusions in sensitive areas. We leverage strong algorithms to teach computers to differentiate various drone intrusions. By employing algorithms capable of detecting minor patterns indicative of drone presence, and utilizing a large dataset encompassing representations of common intrusion scenarios, including unauthorized flights and security breaches, we train these algorithms effectively. This approach not only provides fast and accurate detection of drone intrusions but also serves as an early warning system for farmers and security personnel, alerting them to potential threats and optimal times to take preventive measures. By deploying this technology, we aim to empower communities reliant on security to safeguard their interests, ensuring the protection of critical assets and minimizing potential risks posed by unauthorized drone activities.

I. INTRODUCTION

Drone tracking and detection using real-time data analytics frameworks is the focus of deep learning-based drone intrusion detection. Technologies like decision makers, data collectors, centralized RNNs, and recurrent neural networks (RNN) enhance these systems' ability to detect intrusions. Drone intrusion detection using deep learning is a rapidly developing field in unmanned aerial vehicle (UAV) surveillance. Real-time drone detection and classification is achieved through the use of DL algorithms such as CNNs.

By enabling effective drone surveillance and tracking using cameras and other sensors, deep learning in computer vision—more specifically, convolutional neural networks (CNNs)—has revolutionized drone detection. Modern drone detection models and training techniques are the main focus of this field's research, which aims to solve problems like real-time, long-range detection of tiny drones.

As drone usage increases and the demand for dependable and efficient drone detection systems grows, deep learning-based drone detection system development is essential. In order to provide a clear picture of the airspace and guarantee the safety and security of people, property, and vital infrastructure, these systems can be integrated with other surveillance systems.

These systems, which combine deep learning and optics, improve security measures against potential drone threats by effectively detecting, tracking, and identifying UAVs. Compared to conventional techniques, deep learning for drone detection has a number of benefits. It can identify the distinctive features of drones by being trained on sizable datasets, making it possible to detect drones even when they are partially obscured or photographed from different angles. Additionally, deep learning models can be improved to catch tiny drones and accurately identify them in real time.

II. LITERATURE REVIEW

Rui Fu Et al [1]. The study's primary foci are data encryption in intelligent farming and the safe process of agricultural information in systems. In the context of the Agricultural Internet of Things, it suggests a double Q-network algorithm for location processing and combines CNN and LSTM for intrusion detection.

Shangting Miao Et al [2]. The primary focus of the research is data encryption in intelligent farming and the safe execution of agricultural information in systems. CNN and LSTM are combined for intrusion detection, and a double Q-network algorithm is suggested for place processing in the framework of the Agricultural Internet of Things.

M. Sivachandran Et al [3]. The study ranked Multilayer Perceptron as the most accurate, precision-rich, and time-efficient approach, surpassing Gaussian Processes, Linear Regression, Logistic, and SGD methods, with Gaussian Processes achieving the highest recall value.

Ruohao Zhang Et al [4]. The study presents a novel algorithm to detect phishing attacks in UAV location complaining systems using machine learning and wavelet leader multifractal analysis (WLM). The algorithm emphasizes the significance of network security in UAS operations by striving to improve IDS methodology and offer a strong approach with low false positives. The use of LSTM networks for signature classification is also covered in the study.

Rabie A. Ramadan Et al [5]. In order to analyze data from multiple sources, such as operating system services, and network systems, the study suggests a coordinated architecture. It suggests a local intrusion detection system for drone networks and uses deep learning algorithms to assess the framework's performance. The study highlights how crucial it is to improve intrusion detection systems in order to conduct UAV operations.

Qasem Abu Al-Haija Et al [6]. In order to identify harmful threats in UAV communication networks, the study presents an automatic intrusion identification system called UAV-IDS-ConvNet using deep CNN. The system's efficacy in safeguarding UAV communication networks is demonstrated by its ability to outperform current intrusion detection systems by 6-23% using secured internet data from three different types of UASs.

V. Praveena Eta al [7] talks about In order to improve intrusion identification performance in UAS networks, the DRL-BWO algorithm—a deep belief network based on reinforcement learning—is suggested. It achieves high values for accuracy, precision, recall, and F-measure.

Boban Sazdi´c-Joti´c Et al [8]. In the study, a DL algorithm to identify the single and multiple drones is evaluated, and a new dataset for RF UAV signals is created. It investigates the effects of additive white Gaussian noise and propagation on the accuracy. The algorithm outperforms other methods, demonstrating the importance of efficient algorithms.

Said Ouiazzane et al [9]. proposes a novel method that addresses security flaws in ad hoc networks by using a more-agent system for intrusion detection in UAS networks. The system's autonomous agents are responsible for improving drone fleet security through real-time detection, alert management, reporting, and action in the event of an attack.

Syed Samiul Alam Et al [10]. The study presents a deep learning model that uses radio frequency signatures for real-time UAV identification and detection. This model outperforms previous approaches in terms of accuracy and inference time since it employs multiscale feature-extraction techniques without the need for human intervention.

Jason Whelan Et al [11]. The study talks about using flight logs to detect attacks using PCA and one-class classifiers. It successfully detects and mitigates attacks even when jamming is occurring by integrating IDS into MAVIDS, a system installed on UAVs.

Jing Tao Eta al [12]. The paper addresses the security issues surrounding unmanned aerial vehicles (UAVs) and suggests using deep reinforcement learning to identify and stop attacks on UAV aerial computing networks. Potential uses in monitoring, sensing, and logistics are highlighted, and the significance of combining mobile edge computing and intrusion detection is underlined.

Hind Bangui Et al [13] The survey addresses the application of machine learning to intrusion detection systems in the transportation industry, with a focus on UAV-assisted networks and vehicular ad hoc networks. It emphasizes how crucial it is to have trustworthy systems in place to identify and stop cyberattacks, addresses security issues, and recommends working together among Intrusion Detection Systems (IDSs) to guarantee data security, justice, and trust.

Mohammad Ashiqur Rahman et al [14] The study suggests using ML -based intrusion detection systems to identify hacked power electronics in unmanned aerial vehicles (UAVs), handle malicious data, and execute control commands to guarantee security in real time.

Ruohao Zhang Et al [15] The AMDES algorithm is a novel approach designed to identify spoofing attacks in unmanned aerial systems (UAS) networks. It combines machine learning and wavelet leader multifractal analysis. This strong approach tackles IoE network security issues and prioritizes secure communication networks for UAS compliance and cyber threat defense.

Yating Liu [16]. The AMDES algorithm, a novel method for detecting spoofing attacks in unmanned aerial systems, uses wavelet leader multifractal analysis and machine learning to

reduce false positives, improve accessibility, and address ethical considerations.

III. METHODODLOGY

Dataset and Features Description:

Our Dataset contains 4000 images of Drones and bird images.

Training: Validation: Testing = 60:20:20

Class	Training	Val	Testing
Drones	1400	460	460
Birds	1400	460	460

Table – 1 Data Split

Collect a dataset drones and birds. Ensure that the dataset is diverse and representative of the variations in maize leaf diseases. Split the dataset into training and testing sets. Resize the images to a consistent size (200x200 pixels). zoom range=0.15, width_shift_range=0.2, shear range=0.15. Freeze the layers of the base model and add custom layers on top for fine-tuning.

CNN:

The methodology outlines the creation of a convolutional neural network (CNN) for image classification using Keras. The model is defined sequentially, starting with convolutional layers and max-pooling layers. The convolutional layers use 3x3 filters and rectified linear unit activation functions. The feature maps are flattened into a 1D array, and two dense layers are added, each with 128 units and ReLU activation. A model summary is printed to display the architecture and parameter details.

RESNET:

The methodology involves importing a pre-trained ResNet50 model from Keras applications, adding custom classification layers, passing the output through a global average pooling layer, adding a dense layer with 1024 units and ReLU activation for higher-level features, and adding a dense layer with 2 units and softmax activation for binary classification. The resulting model is constructed using the Functional API, with the inputs from the ResNet50 base model and outputs from the custom classification layers.

DENSENET:

The methodology involves adding custom classification layers to an existing base model, pre-trained on the ImageNet dataset. The output features are reduced using a global average pooling layer, a dense layer with 1024 units and ReLU activation for higher-level features, and a dense layer with 2 units and softmax activation for binary classification. The resulting model is constructed using the Functional API, with the model summary providing an overview of architecture and parameter details.

INCEPTION:

The methodology uses the InceptionV3 pre-trained model from Keras, with weights pre-loaded from the ImageNet dataset. Custom binary classification layers are added to the base model. A function named main_model is defined, taking input parameters like the transfer learning model and class number. The model is outputted, followed by a global average pooling layer, dense layers with 1024, 512, and ReLU activation functions, and a dense layer with softmax activation for binary classification.

Self-Attention:

We are using multi-head attention Mechanism. Multi-head attention includes an inventory mechanism of different heads (heads of attention) which, in transformer- based architectures, serve the purpose of capturing all the disparities that can exist in sequence inputs. Every day new attention head finds its own multi-level attention signatures by independently making attention scores for projected query, key, and value vectors.

These scores are for the sake of computing weighted sums of values vector from multi-head attention output vector for the specific position in the sequence. Through simultaneously considering different representations of information from multiple subspaces, this kind of attention enables the model to efficiently learn how to understand and process the complex sequences like any natural language text, which, in turn, results in improved accuracy of tasks like machine translation, text classification, and language generation.

1. **num_heads:** specifies the number of parallel attention heads to use in the multi-head attention mechanism. This allows the model to capture a variety of patterns and relationships present in the input data all at the same time. Adjusting the num_heads would impact how the model learns and processes information from these different perspectives. The higher the value of num_heads, the more aspects of the input the model can attend to at the same time, possibly improving the performance, at the cost of higher computational complexity.
2. **key_dim:** This is the dimensionality for both the projected key and value vectors across each attention head. That is, it explains the granularity of captured information in each head and, through this, the model's ability to understand relationships between tokens. The key_dim should be large enough to capture meaningful information but small enough to make the computation efficient. Typical values for key_dim are between 64 and 512, but the best choice depends on the complexity of the task and the resources available.

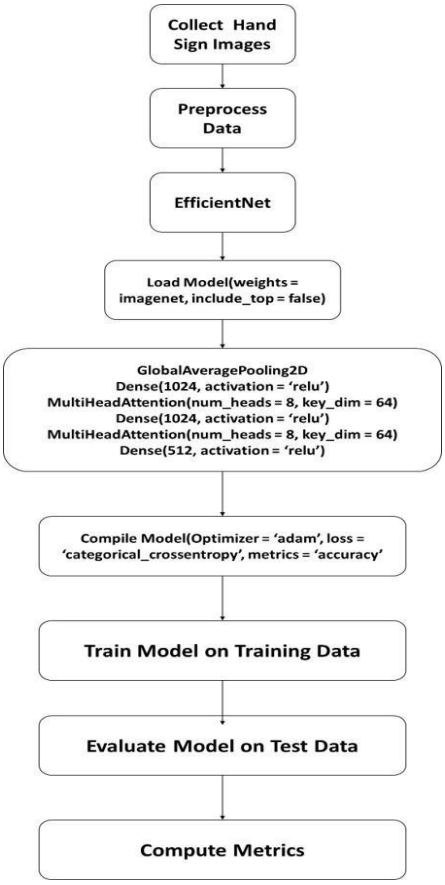

Fig 1. Model Architecture

IV. EXPERIMENTS

Model	Batch Size	Image Dimensions	Activation Function	Optimizer
CNN	32	256 X 256	Relu, Softmax	Adam
Resnet	32	256 X 256	Relu, Softmax	Adam
Dense	32	256 X 256	Relu, Softmax	Adam
Inception	32	256 X 256	Relu, Softmax	Adam

Table -2 Parameters of the Model

Model	Epochs	Loss Function	Metrics
CNN	50	Categorical Cross Entropy	Accuracy
Resnet	50	Categorical Cross Entropy	Accuracy
Dense	50	Categorical Cross Entropy	Accuracy
Inception	50	Categorical Cross Entropy	Accuracy

Table -2 Parameters of the Model (Cont...)

This table details the parameters for training a deep learning model. The dataset is split into 60% for training, 20% for validation, and 20% for testing. Images are resized to 256x256 pixels and processed in batches of 32. ReLU is used as the activation function in hidden layers, and Softmax in the output layer. The Adam optimizer adjusts model parameters to minimize the categorical crossentropy loss function. Model performance is evaluated using accuracy. The number of steps per epoch is calculated by dividing the total number of images by the batch size.

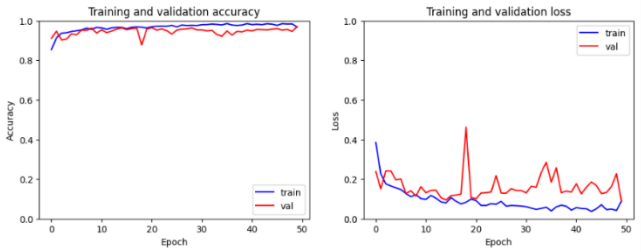

Fig 2. Training and Validation Accuracy & Loss of Inception (No Self Attention Layers)

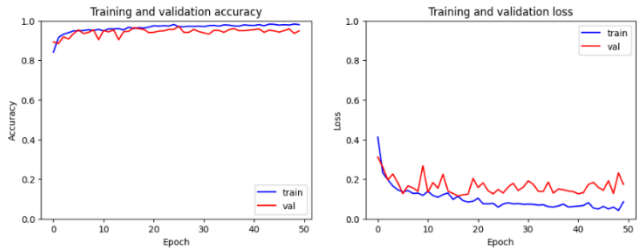

Fig 3. Training and Validation Accuracy & Loss of Inception-1

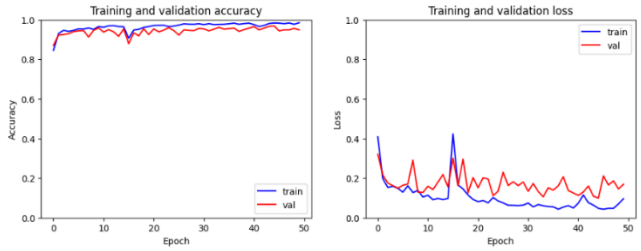

Fig 4. Training and Validation Accuracy & Loss of Inception-2

V. RESULTS

Model	Acc	Pre	F1	Rec
CNN	93.4	89.95	93.02	94.02
Dense Net 50	94.41	87.89	95.12	94.42
Res Net 50	93.46	89.66	93.89	90.79
Inception	**96.83**	**94.77**	**96.94**	**84.94**

Table 3. Evaluation Metrics

From Table 3, The table compares several deep learning models for classification tasks, with InceptionV3 emerging as the best performer. It achieves the highest scores in Precision (0.9477), Recall (0.8494), F1 Score (0.9694), and Accuracy (0.9683). This indicates that EfficientNetB4 excels in accurately identifying true positives while minimizing false positives, making it the most effective model overall.

Model	Loss	Acc	Val_L	Val_acc
CNN	0.2357	0.8981	0.5635	0.7789
DENSENET	0.0273	0.9950	0.2599	0.8953
RESNET	0.4349	0.8171	0.4972	0.7708
INCEPTION	**0.0141**	**0.9952**	**0.1784**	**0.9296**

Table 4. Training and Validation Metrics

One of the added attention layers in the multihead layers to InceptionV3 which helped to achieve the highest Accuracy and F1 Score. The multihead attention layers improve the alignment of the model on the parts of data which help the model to focus on the data parts and extract features better and improves the performance of the model overall.

Models	Accuracy		
	Train	Val	Test
Inception	93.22	85.11	96.83
Inception (Layer 1)	95.05	94.27	96.89
Inception (Layer 2)	96.88	98.99	97.67

Table 5. Evaluation Metrics – InceptionV3

Table -5 shows the Train accuracy, Validation Accuracy and test accuracy of the models Inception, Inception(Layer-1), Inception(Layer-2) in those three we achieved higher metric when we tested for Inception(Layer 2)

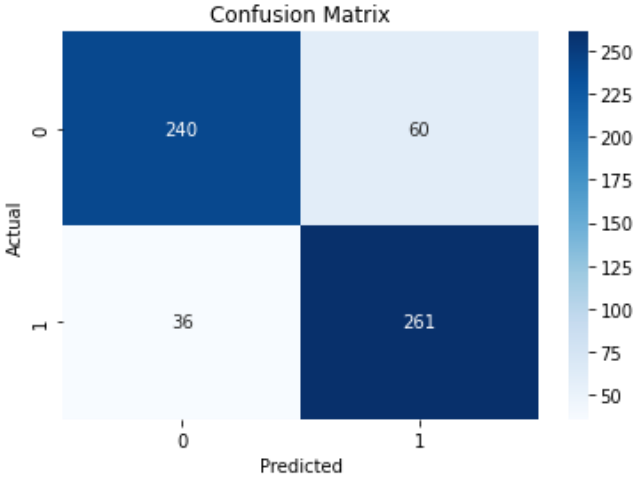

Fig 4. Confusion Matrix Inception-1

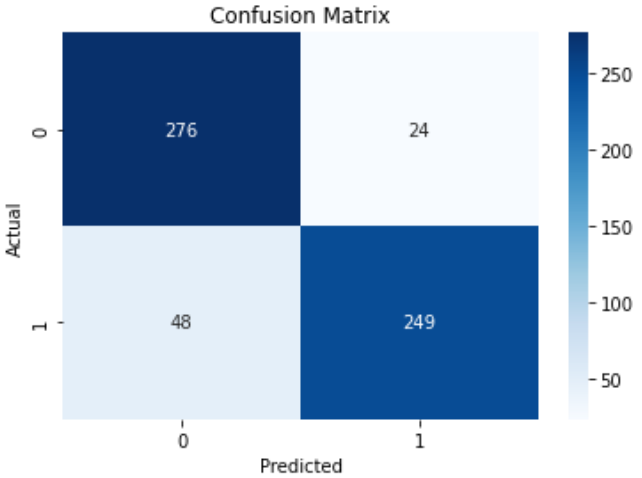

Fig 4. Confusion Matrix Inception-2

VI. Conclusion

In summary, the dense layers and self-attention mechanisms integrated into the architecture of InceptionV3 result in the derived equivalent increase in the efficiency of drone intrusion detection. We observed a dramatic change in accuracy and robustness associated with model capabilities after a host of experiments. Added depth to the learned features through dense layers, thus allowing the distinction between normal and intrusive drone activities. More importantly, the addition of self-attention mechanisms turned the model into an effective way of focusing on different regions in an input image adaptively, where that attention improves interpretability and decision-making. We demonstrated here how state-of-the-art deep learning techniques could be used for increasing the efficiency of security practices in general and early detection of drone intrusions and the effective management of airspace.

References

[1] Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H. and Al-Absi, M.A., 2023. Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. IEEE Internet of Things Journal.

[2] Miao, S., Pan, Q. and Zheng, D., 2024. Unmanned aerial vehicle intrusion detection: Deep-meta-heuristic system. Vehicular Communications, 46, p.100726.

[3] Sivachandran, M. and Krishnakumar, T., 2022. Classification approaches in unmanned aerial vehicle (uav) intrusion detection data set by using big data analysis. Materials Today: Proceedings, 51, pp.1129-1133.

[4] Zhang, R., Condomines, J.P. and Lochin, E., 2022. A multifractal analysis and machine learning based intrusion detection system with an application in a UAS/RADAR system. Drones, 6(1), p.21.

[5] Ramadan, R.A., Emara, A.H., Al-Sarem, M. and Elhamahmy, M., 2021. Internet of drones intrusion detection using deep learning. Electronics, 10(21), p.2633.

[6] Abu Al-Haija, Q. and Al Badawi, A., 2022. High-performance intrusion detection system for networked UAVs via deep learning. Neural Computing and Applications, 34(13), pp.10885-10900.

[7] Praveena, V., Vijayaraj, A., Chinnasamy, P., Ali, I., Alroobaea, R., Alyahyan, S.Y. and Raza, M.A., 2022. Optimal deep reinforcement learning for intrusion detection in UAVs. Computers, Materials & Continua, 70(2), pp.2639-2653.

[8] Sazdić-Jotić, B., Pokrajac, I., Bajčetić, J., Bondžulić, B. and Obradović, D., 2022. Single and multiple drones detection and identification using RF based deep learning algorithm. Expert Systems with Applications, 187, p.115928.

[9] Ouiazzane, S., BarramoU, F. and Addou, M., 2020. Towards a multi-agent based network intrusion detection system for a fleet of drones. International Journal of Advanced Computer Science and Applications, 11(10).

[10] Alam, S.S., Chakma, A., Rahman, M.H., Bin Mofidul, R., Alam, M.M., Utama, I.B.K.Y. and Jang, Y.M., 2023. RF-Enabled Deep-Learning-Assisted Drone Detection and Identification: An End-to-End Approach. Sensors, 23(9), p.4202.

[11] Whelan, J., Almehmadi, A. and El-Khatib, K., 2022. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. Computers and Electrical Engineering, 99, p.107784.

[12] Tao, J., Han, T. and Li, R., 2021. Deep-reinforcement-learning-based intrusion detection in aerial computing networks. IEEE Network, 35(4), pp.66-72.

[13] Bangui, H. and Buhnova, B., 2021. Recent advances in machine-learning driven intrusion detection in transportation: Survey. Procedia Computer Science, 184, pp.877-886.

[14] Rahman, M.A., Rahman, M.T., Kisacikoglu, M. and Akkaya, K., 2020, October. Intrusion detection systems-enabled power electronics for unmanned aerial vehicles. In 2020 IEEE CyberPELS (CyberPELS) (pp. 1-5). IEEE.

[15] Ruohao, Z., Condomines, J.P. and Lochin, E., 2022. A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. Drones 2022, 6, 21.

[16] Liu, Y., 2023. Drone Detection using Deep Learning.

[17] Wang, Y., Ding, J., He, X., Wei, Q., Yuan, S. and Zhang, J., 2023. Intrusion Detection Method Based on Denoising Diffusion Probabilistic Models for UAV Networks. Mobile Networks and Applications, pp.1-10.

[18] Mojib, E.B.S., Haque, A.B., Raihan, M.N., Rahman, M. and Alam, F.B., 2019, November. A novel approach for border security; surveillance drone with live intrusion monitoring. In 2019 IEEE international conference on robotics, automation, artificial-intelligence and internet-of-things (RAAICON) (pp. 65-68). IEEE.

[19] Abdulghani, A.M., Abdulghani, M.M., Walters, W.L. and Abed, K.H., 2022. Improving Intrusion Detection in UAV Communication Using an LSTM-SMOTE Classification Method. Journal of Cybersecurity (2579-0072), 4(4).