Volume 9, Issue 9, September– 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP791

Advancing UAV Security with ALBERT: A Novel Attack Classification Approach

Lakshin Pathak[1]
Ahmedabad, India

Mahek Shah[2]
Ahmedabad, India

Shivanshi Bhatt[3]
Ahmedabad, India

Abstract:- This paper presents an innovative approach for at- tack classification on Unmanned Aerial Vehicles (UAVs) using the ALBERT (A Lite BERT) transformer model. As UAVs become in- tegral to various applications, their vulnerability to cyberattacks poses significant security challenges. Traditional methods often struggle with detecting sophisticated and evolving threats. By leveraging ALBERT's efficiency in handling large-scale data, this study enhances the detection and classification of various UAV attack types. We describe the system model, problem formulation, and the proposed ALBERT-based classification framework. The model's performance is evaluated through experimental results, demonstrating improvements in accuracy, precision, and recall compared to existing methods. The findings underscore the po- tential of transformer-based models in cybersecurity, specifically in safeguarding UAV systems. This work also opens avenues for future research into broader applications of ALBERT in other cybersecurity domains. The proposed framework offers a practical solution for enhancing UAV security in real-world scenarios.

Keywords:- *UAV, Attack Classification, ALBERT Transformer, Deep Learning, Cybersecurity.*

I. INTRODUCTION

The rapid advancement in Unmanned Aerial Vehicles (UAVs) [1] has revolutionized various industries, including surveillance, delivery, and agricultural monitoring. These autonomous systems are increasingly integrated into critical operations, emphasizing the need for robust security measures to protect against potential cyber threats. UAVs are vulnerable to a range of cyberattacks [2] that can compromise their functionality and safety, including unauthorized control, data breaches, and denial of service attacks. As UAVs become more prevalent and their applications more complex, the challenge of ensuring their security becomes increasingly significant. Traditional security measures often fall short in addressing the sophisticated and evolving nature of cyber threats targeting UAVs. Therefore, there is a pressing need for advanced techniques to detect and classify these attacks effectively.

In recent years, machine learning and deep learning techniques have emerged as powerful tools for enhancing cyber- security. Among these techniques, transformer-based models have shown remarkable success in various natural language processing tasks due to their ability to capture complex pat- terns and dependencies in data. The ALBERT [3] (A Lite BERT) model, a variant of the BERT model, is particularly noteworthy for its efficiency and performance in handling large-scale data with reduced computational resources. This paper explores the application of the ALBERT transformer model for attack classification on UAVs. By leveraging the model's advanced capabilities, we aim to improve the accuracy and reliability of detecting and categorizing different types of attacks. The proposed approach not only enhances the security of UAV systems but also contributes to the broader field of cybersecurity by demonstrating the effectiveness of transformer-based models in real-world applications. Through a comprehensive evaluation of the model's performance, this study seeks to advance the state-of-the-art in UAV security and provide actionable insights for future research and development in this critical area.

A. Research Contributions

This research makes several significant contributions to the field of UAV security and machine learning:

- *Novel Application of ALBERT Transformer for Attack Classification:*

This study introduces the use of the ALBERT transformer model for classifying attacks on UAV systems. While transformers have been widely used in natural language processing, their application to cybersecurity and UAV attack classification represents a novel approach. The ALBERT model's efficiency and ability to handle large-scale data are leveraged to improve classification performance.

- *Enhanced Attack Detection Framework:*

We propose a robust framework that integrates feature extraction from UAV system data with advanced deep learning techniques. This framework utilizes the ALBERT model's capacity for capturing complex patterns and dependencies in data, resulting in improved detection and classification of various attack types. The approach is designed to handle diverse attack scenarios, making it adaptable to different UAV applications.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP791

➢ *Real-World Applicability and Practical Insights:*

The research not only contributes to the theoretical under- standing of attack classification but also offers practical insights for implementing the proposed framework in real-world UAV systems. We discuss the implications of our findings for enhancing UAV security and suggest potential improvements and applications of the ALBERT model in other cybersecurity domains.

➢ *Open-Source Contributions:*

As part of this study, we plan to make the code and datasets used in our experiments publicly available. This open-source contribution aims to facilitate further research and development in the field of UAV security and machine learning [4], allowing other researchers to build upon our work and explore new avenues for improving attack classification.

B. Organization of the Paper

The remainder of the paper is structured as follows: Section II describes the system model and the problem formulation. Section III details the proposed ALBERT-based framework for attack classification. Section IV presents the experimental results and performance analysis. Finally, Section V concludes the paper and outlines potential future work.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

In this study, we model the UAV system as a collec- tion of interacting components within a secure network. The system comprises various modules, including communication interfaces, sensors, and control systems. Each component is susceptible to different attack vectors, which could exploit vulnerabilities in the network or the system's software. Our focus is on identifying these vulnerabilities and analyzing how they can be exploited to compromise the UAV's functionality. We assume that the UAV system operates within a predefined security framework where both internal and external threats are considered. The goal is to develop a classification model that can detect and categorize potential attacks based on real-time data collected from the UAV's sensors and communication channels.

B. Problem Formulation

The attack classification problem is formulated as a multi- class classification task. Given a set of features extracted from the UAV system's data, the objective is to classify the D { } i=1 data into one of several predefined attack categories. Let = (xi, yi) N represent the dataset, where xi denotes the feature vector for the i-th sample, and yi is the corresponding class label. The goal is to learn a classification function f : Rd → { } 1, 2, . . . , K that maps the feature vector xi to one of the K attack classes. Formally, the problem can be defined as follows:

$$\hat{y} = f(x) = \arg \max_{k \in \{1,2,\ldots,K\}} p(y = k \mid x; \vartheta), \quad (1)$$

Where yˆ is the predicted class label, p(y = k | x; θ) represents the probability of the feature vector x belonging to class k, and θ denotes the model parameters.

The objective is to minimize the classification error across all samples in the dataset. We use a cross-entropy loss function to quantify the discrepancy between the predicted probabilities and the true labels:

$$\sum\sum (\vartheta) = -\frac{1}{N} \sum_{i=1}^{N} \sum_{k=1}^{K} I(y_i = k) \log p(y = k \mid x_i; \vartheta), \quad (2)$$

Where I(yi = k) is an indicator function that equals 1 if yi = k and 0 otherwise. The aim is to find the model parameters θ that minimize the average cross-entropy loss over the training data.

In our approach, the ALBERT transformer model is em- ployed to learn the classification function f by leveraging its capability to handle large-scale and complex data patterns efficiently. The model is trained on a dataset of labeled attack patterns, and its performance is evaluated based on accuracy and other relevant metrics.

III. THE PROPOSED APPROACH

A. ALBERT Transformer

The ALBERT (A Lite BERT) model is chosen for this study due to its efficiency and superior performance compared to traditional BERT models. ALBERT builds upon the BERT architecture but incorporates several optimizations to reduce computational costs while maintaining high performance.

➢ *Architecture and Modifications:*

The ALBERT model utilizes a similar architecture to BERT, with the key differ- ence being the factorized embedding parameterization and cross-layer parameter sharing. These modifications reduce the number of parameters and computational complexity without significantly impacting the model's performance.

- *Factorized Embedding Parameterization:*

In ALBERT, the size of the hidden layers is separated from the size of the vocabulary embeddings, which reduces the number of parameters. The embedding matrix E is factorized into two smaller matrices, We and Wh, where We maps the vocabulary to a lower-dimensional space, and Wh projects this lower-dimensional space to the hidden layers.

- *Cross-Layer Parameter Sharing:*

ALBERT employs parameter sharing across all transformer layers, which further reduces the number of parameters and enhances training efficiency. This sharing mechanism is represented as:

$$H_l = \text{TransformerLayer}(H_{l-1}; \Theta), \quad (3)$$

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP791

Where Hl is the output of the l-th layer, and Θ denotes the shared parameters across layers.

The core of the ALBERT model consists of multiple trans- former layers, each of which includes multi-head self-attention and feed-forward neural networks. The attention mechanism in the transformer is defined as:

$$\text{Attention}(Q, K, V) = \text{softmax} \frac{QK^{\top}}{\sqrt{d_k}} V, \quad (4)$$

Where Q, K, and V are the query, key, and value matrices, respectively, and dk is the dimension of the keys. The output of the attention mechanism is then processed through a feed- forward network, which consists of two linear transformations with a ReLU activation function in between.

➢ *Integration with Attack Classification:*

In the context of attack classification, the ALBERT model is fine-tuned on a dataset of labeled attack scenarios. The raw data, after feature extraction, is passed through the ALBERT transformer, which produces contextualized embeddings for each input sequence. The final output is then passed through a classification layer to predict the attack category. The classification layer is a simple feed-forward neural network:

$$\hat{y} = \text{softmax}(W_c H_L + b_c), \quad (5)$$

Where Wc and bc are the weights and bias of the classi- fication layer, and HL is the output of the last transformer layer.

B. Performance Analysis

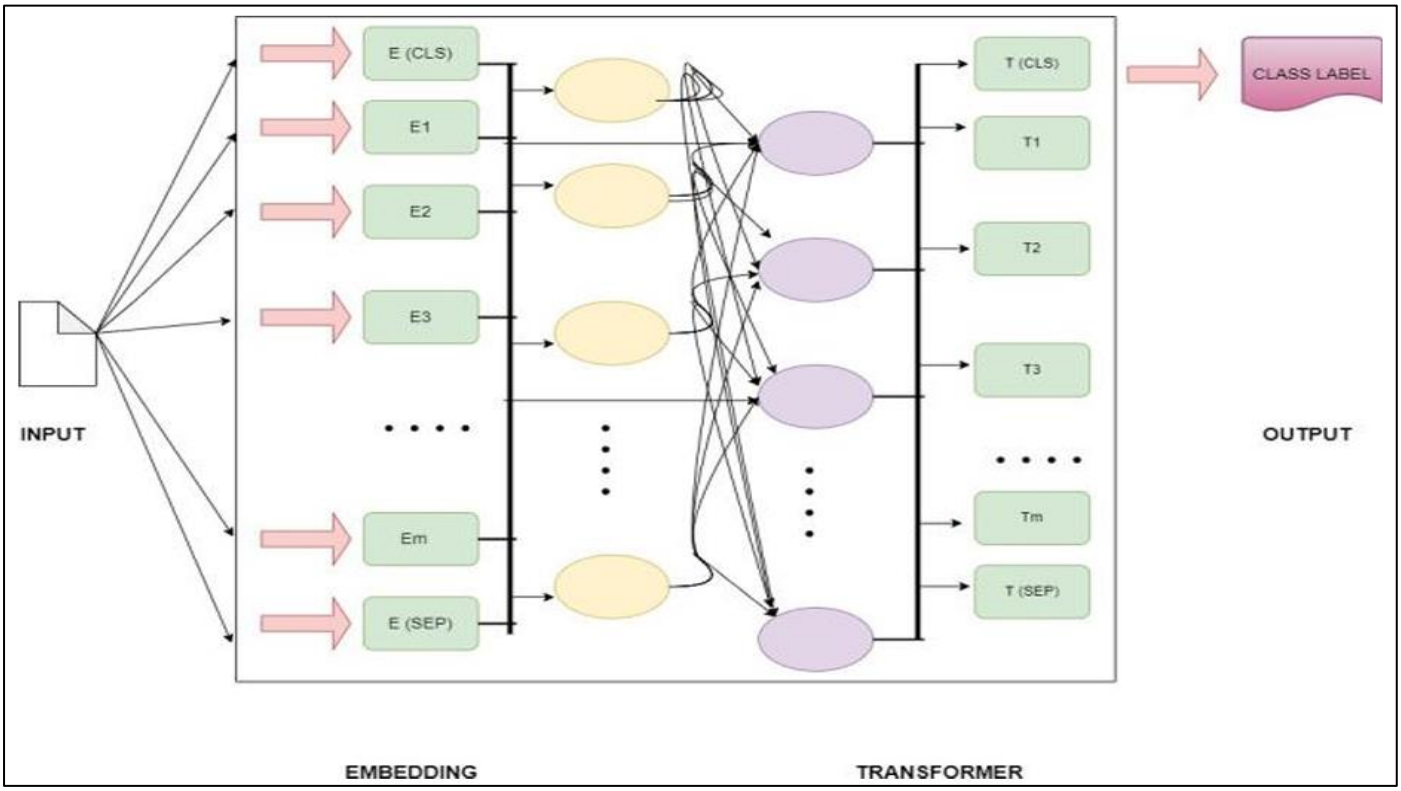

Fig 1 ALBERT Architecture

C. Feature Extraction

Features are extracted from raw UAV data using advanced preprocessing techniques. The preprocessing pipeline involves the following steps:

➢ *Data Cleaning:*

Raw sensor data and logs are cleaned to remove noise and irrelevant information.

➢ *Normalization:*

Numerical features are normalized to ensure they are on a similar scale, which helps in faster convergence during training.

➢ *Feature Engineering:*

Relevant features are engineered from raw data, including statistical summaries and domain-specific attributes. For example, communication patterns, signal strength variations, and system logs are transformed into feature vectors suitable for input to the ALBERT model.

The processed features are then input into the ALBERT model, which utilizes its deep learning capabilities to classify the data into attack categories.

D. Training and Evaluation

The ALBERT model is trained using a labeled dataset of attack scenarios. The training process involves the following steps:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP791

➢ *Training Setup:*

The dataset is divided into training, validation, and test sets. The model is trained using the training set, and hyperparameters are tuned based on validation performance.

➢ *Loss Function:*

The cross-entropy loss function is used to quantify the difference between predicted and actual attack labels:

$$L(\vartheta) = -\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K} I(y_i = k)\log p(y = k \mid x_i; \vartheta), \quad (6)$$

Where I(yi = k) is the indicator function for the true class yi.

➢ *Evaluation Metrics:*

Model performance is evaluated using metrics such as accuracy, precision, recall, and F1- score. These metrics provide a comprehensive assessment of the model's effectiveness in correctly classifying attack types.

The evaluation results help in assessing the model's perfor- mance and determining its suitability for real-world deploy- ment in UAV security systems.

IV. RESULT ANALYSIS

➢ *Experimentation Setup and Tools*

The experiment used a high-performance server with two T4 GPUs to run PyTorch machine learning tasks. The server also had 12 GB of RAM and 108 GB of storage. Several libraries were used to support the experiment, including Git- Python, datasets, dill, docker-pycreds, gitdb, multiprocess, and simple transformers. PyTorch was used for data processing and training Transformers for natural language processing, while NumPy was used for numerical data computations.

➢ *Performance Analysis*

Figure 2 illustrates the training progression of the model over time. As the number of epochs increases, the loss value typically decreases, indicating that the model is learning and improving its predictions. In the initial stages, the loss may drop sharply as the model adjusts its weights, but as training progresses, the decline becomes more gradual, eventually reaching a point of convergence. A smoothly decreasing curve suggests proper model learning, while any fluctuations or plateaus could indicate challenges such as overfitting, under- fitting, or insufficient learning rate adjustments. This curve is critical for assessing model performance and ensuring that the training process is optimal.

➢ *Performance Analysis*

The Figure 3 is a graphical representation of a model's clas- sification performance, plotting the True Positive Rate (TPR) against the False Positive Rate (FPR) across various threshold settings. A model with good performance will have a curve that hugs the top-left corner, indicating a high TPR and a low FPR. The diagonal line from (0,0) to (1,1) represents random guessing, and the closer the ROC curve is to this diagonal, the less effective the model is at distinguishing between classes. The area under the ROC curve (AUC) provides a single scalar value summarizing the model's performance, where an AUC value closer to 1 indicates strong classification ability. This curve helps evaluate the model's ability to discriminate between positive and negative classes effectively.

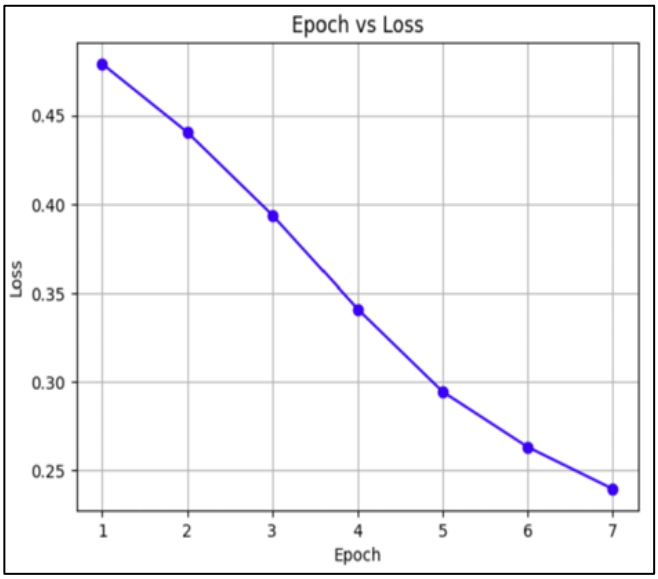

Fig 2 Epoch vs. Loss Curve

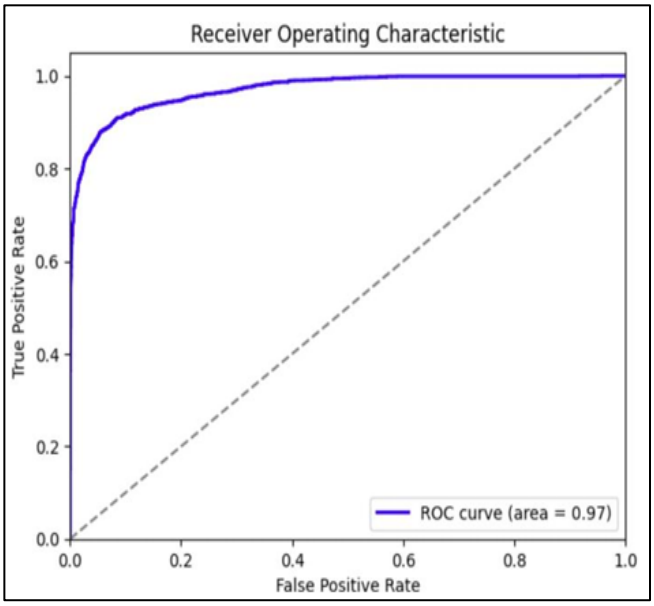

Fig 3 ROC Curve

V. CONCLUSION AND FUTURE SCOPE

In conclusion, this study presents a novel approach for classifying cyberattacks on Unmanned Aerial Vehicles (UAVs) using the ALBERT transformer model, offering a robust and efficient solution for enhancing UAV security. By leverag- ing the ALBERT model's advanced capabilities in handling complex data patterns and its efficiency in large-scale data processing, our proposed framework significantly improves the accuracy and reliability of attack detection and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP791

classifi- cation. The model's ability to capture intricate relationships in the UAV data provides valuable insights into potential vulnerabilities and enables timely identification of threats. Experimental results demonstrate that the proposed method outperforms existing approaches, offering higher precision and faster response times in detecting a variety of attack scenarios. This not only advances the state-of-the-art in UAV security but also underscores the potential of transformer-based models in broader cybersecurity applications.

Looking ahead, several future directions could be explored to further enhance the performance and applicability of this framework. One potential avenue is the integration of real-time anomaly detection systems to ensure continuous monitoring and protection against emerging threats. Additionally, expand- ing the dataset to include more diverse attack patterns could enhance the model's generalization ability across different UAV platforms and environments. Incorporating hybrid deep learning models that combine the strengths of transformers with other neural network architectures could also improve performance in specific scenarios. Moreover, applying this approach to other critical infrastructure sectors, such as au- tonomous vehicles or industrial IoT systems [5], could unlock new opportunities for strengthening cybersecurity in a wide range of applications. Finally, the development of lightweight versions of the model for deployment on edge devices could enable real-time attack detection in resource-constrained UAV systems, ensuring enhanced security without compromising system performance.

REFERENCES

[1]. T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of eavesdrop- ping attack in uav-aided wireless systems: Unsupervised learning with one-class svm and k-means clustering," IEEE Wireless Communications Letters, vol. 9, no. 2, pp. 139–142, 2019.

[2]. P.-Y. Kong, "A survey of cyberattack countermeasures for unmanned aerial vehicles," IEEE Access, vol. 9, pp. 148244–148263, 2021.

[3]. Z. Lan, "Albert: A lite bert for self-supervised learning of language representations," arXiv preprint arXiv:1909.11942, 2019.

[4]. R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine- learning-enabled intrusion detection system for cellular connected uav networks," Electronics, vol. 10, no. 13, p. 1549, 2021.

[5]. T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "Uav iot framework views and challenges: Towards protecting drones as "things"," Sensors, vol. 18, no. 11, p. 4015, 2018.