Deep Learning based Intrusion Detection for Cybersecurity in Unmanned Aerial Vehicles Network

Simon Niyonsaba
Dept.Mathematics and Computer Science
Cheikh Anta Diop University (UCAD)
Dakar, Senegal
simon.niyonsaba@ucad.edu.sn

Karim Konate
Dept. Mathematics and Computer Science
Cheikh Anta Diop University (UCAD)
Dakar, Senegal
karim.konate@ucad.edu.sn

Moussa Moindze Soidridine
Dept. Mathematics and Computer Science
Cheikh Anta Diop University (UCAD)
Dakar, Senegal
moussa.soidridine@ucad.edu.sn

2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) | 979-8-3503-9591-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICECET61485.2024.10698453

***Abstract*—In this article, we have proposed Deep Learning techniques for cybersecurity in Unmanned Aerial Vehicles (UAVs). UAVs, also known as drones, have become versatile tools used in many applications. However, UAV cybersecurity remains a major concern due to the evolution of cyberattacks. Faced with this issue, it is important to give a contribution on intrusion detection systems (IDS) to be applied in UAVs, given that existing cybersecurity solutions still present limitations. It is in this context that we have proposed Deep Learning-based intrusion detection models such as Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and the combination of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models (CNN+LSTM) and these are evaluated using the CICIDS2017 dataset. Based on their performance, the proposed models are compared with Machine Learning models to decide on the best model for intrusion detection in UAVs. Thus, the results obtained during the experiment indicate that the hybrid CNN-LSTM model obtained a high accuracy of 99.063% compared to the other models.**

Keywords—UAV, Cybersecurity, Deep Learning, Machine Learning, CNN, LSTM, LR, NB, cyberattacks, CICIDS2017

I. INTRODUCTION

The advent of the Internet has brought major developments in various areas of society, paving the way for global connectivity and new technological opportunities. Unmanned Aerial Vehicles (UAVs), also known as drones, are one of the technologies benefiting from the advantages of the Internet. They are widely used in both civil (agriculture, logistics, mapping, disaster management, commerce, etc.) and military (reconnaissance, intelligence, blast detection, border surveillance, combat, etc.) applications [1]. However, UAV security remains a major challenge, as UAVs are exposed to numerous security risks. The security risks to which UAVs are exposed are numerous [2]. They can be DDoS/DoS attacks, infiltration attacks, brute force attacks, SQL injection, etc., which today represent serious threats to data confidentiality, integrity and availability [3]. Faced with this problem, the security solutions currently deployed are proving ineffective in the face of the growing sophistication of these various attacks against UAVs, and this ineffectiveness constitutes a major vulnerability that can compromise UAV security. Faced with this problem, the security solutions currently deployed are proving ineffective in the face of the growing sophistication of these various attacks against UAVs, and this ineffectiveness constitutes a major vulnerability that can compromise UAV security. As a result, several intrusion detection systems (IDS) have been developed in general and in particular those based on Machine Learning (ML) and Deep Learning (DL) capable of detecting attacks and suspicious activities [4]. This article focuses on anomaly-based IDS and more specifically on Machine Learning and Deep Learning techniques. Machine Learning algorithms deliver impressive performance due to their learning and training modules. Machine Learning and Deep Learning techniques are more widely used in cybersecurity because they are able to detect both abnormal and normal network or system activity. However, Deep Learning techniques outperform Machine Learning due to their ability to learn more complex data [5]. In addition, Deep Learning techniques do not require feature engineering. Despite this, IDS based on Machine Learning and Deep Learning algorithms require improvement in order to perform better in terms of accuracy. Thus, we propose the IDS model using Convolutional Neural Network (CNN), Long Sort-Term Memory (LSTM), CNN+LSTM, Logistic Regression (LR) and Naive Bayes (NB) algorithms that focus on detecting attacks present in the CICIDS2017 dataset.

This paper aims to:

- Propose Deep Learning models for cybersecurity in UAV networks;
- Evaluate models such as CNN, LSTM, CNN+LSTM, LR and NB using the CICIDS2017 dataset;
- Compare the results of these Machine Learning and Deep Learning models based on performance metrics such as accuracy, precision, recall and F1 Score to decide on the best model for UAV intrusion detection;
- Finally, compare our proposed models with existing models.

The rest of this article is organized as follows: Section II talk about an overview of related work. Section III discuss the Machine Learning and Deep Learning algorithms. Section IV focuses on the methodology used for intrusion detection, the dataset used and their preparation, and the framework of the UAV intrusion detection model. Section V describes the test and experimental environment. Section VI presents the results and discussion. Section VII focuses on conclusions and future work.

II. RELATED WORK

This section presents information on related work carried out in the UAV field. Research [6] has proposed a model based

on the combination of LSTM and SMOTE algorithms that detects intrusions into UAV communications channels. It describes that this approach can be deployed onboard UAVs and at ground control stations, and can also be used to defend communications channels against threats. The approach achieved 99.83% accuracy using the CICIDS2017 dataset. Although the search achieved better results, it does not deal with CNN, although these are important for the extraction of spatial features. In addition, SMOTE can sometimes lead to data overlearning and additional complexity. Therefore, it would be desirable to propose a CNN+LSTM model that benefits from both the advantages of CNN and those of LSTM.
In [7], the authors focus on an IDS based on Machine Learning algorithms for drones connected via various technologies such as 5G and satellite. They use several Machine Learning algorithms to identify benign and malicious packets. Among the algorithms examined, the Decision Tree (DT) algorithm performed best, with an accuracy of 99.9% on the CICIDS2018 dataset.
Despite the results obtained, the Machine Learning algorithms used are considered traditional and feature extraction is done manually. Furthermore, Machine Learning algorithms can be limited when faced with more complex data. It would then be best to examine a hybrid CNN-LSTM model capable of handling complex data and exploiting both the advantages of CNN and LSTM architectures, which can be effective in intrusion detection in general and in UAVs in particular.
The work [8] proposes a Machine Learning-based model that detects DDoS attacks on drones in the Internet of Flying Things (IoFT) network. In this work, three types of DDoS were analyzed. Packets were detected as normal and abnormal using different Machine Learning algorithms such as DT, LR and KNN. To optimize accuracy, a feature selection algorithm was used, achieving 99% accuracy for each type of DDoS attack. Despite these results, traditional Machine Learning algorithms were used. In addition, the suggested model only detects DDoS attacks. In this article, it would be desirable to use Deep Learning algorithms.
A multi-agent network-based intrusion detection model for a drone fleet has been proposed in [9]. The proposed model is based on Machine Learning and consists of a set of agents that collaborate to detect suspicious activity in drones. Despite the best performance obtained (100% accuracy), the authors used a single DT algorithm.
A system based on Deep Learning that detects UAV intrusions was suggested in [10]. Several datasets such as KDDCup99, NSL-KDD, UNSW-NB15, Kyoto, CICIDS2017 and TON_IoT were used to evaluate the model using KNN, LR and the combination of LSTM and Recurrent Neural Networks (RNN) algorithms. According to the experimental results, the model based on the combination of RNN and LSTM algorithms is better than the other models considered, with an average accuracy of 95%. However, most of the packages used are obsolete and the proposed models require improvement.
The study [11] presents a Machine Learning-based model that detects different types of attacks such as DoS attacks, GPS Signal Jamming/Spoofing and Hijacking targeting a drone in a smart city context. Using Machine Learning algorithms, the authors were able to perform a classification of drone data for the DJI Phantom 4 model comprising malicious data and normal signatures. Among the algorithms used for attack detection, Random Forest (RF) was chosen as the best, with an accuracy of 0.984.
Another model for detecting DDoS attacks was proposed in [12] and a combination of CNN and LSTM algorithms was presented. Experimental results show that this combination of CNN and LSTM performs better, with accuracy of 97.16%, than algorithms such as SVM, Bayes and Random Forest. However, the proposed model is designed not to be applicable to UAVs. Furthermore, the work focuses solely on DDoS attacks.

III. MACHINE LEARNING AND DEEP LEARNING ALGORITHMS

Machine Learning, one of the branches of Artificial Intelligence, covers a range of techniques used to solve data-related problems. According to the models developed, Machine Learning is subdivided into three main types detailed in [13]. Deep Learning is the sub-domain of Machine Learning based on artificial neurons. These neurons take data as input, transforming it into values which are then passed on to other neurons. Each type is associated with algorithms used to develop models and perform specific tasks. Among Machine Learning and Deep Learning algorithms, we present the techniques used in this article.

- Logistic Regression (LR): This is a supervised learning algorithm used to perform mainly binary classification tasks. LR is given by the following mathematical equation:

$$Y = 1/\left(1 + e^{-(\beta_o + X\beta)}\right) \quad (1)$$

with Y representing the expected output, β_o is the intercept term, β is the coefficient associated with X, e is the neperian logarithm base, X represents the input characteristic.

- Naïve Bayes (NB): Naïve Bayes is a supervised learning algorithm based on a conditional probability model. NB classifies data according to their properties and probability distribution. This algorithm is based on the following Bayes theorem:

$$P(H|Y) = \frac{P(H)P(Y|H)}{P(Y)} \quad (2)$$

$P(H|Y)$ represents the conditional probability of H knowing the features Y; $P(Y|H)$ is the conditional probability of the features Y knowing that the class H.

- Convolutional Neural Network (CNN): is a class of deep neural networks used in many fields to achieve better performance [14]. CNNs have an architecture composed of several elements such as the input layer, the hidden layers and the output layer giving the prediction results. The hidden layers are the

convolution layer, the activation layer (ReLU), the pooling layer and the Fully Connected Layer [15]. The convolution process is represented as follows:

$$C(t) = \sum_b F\,(t+b).k(b) \qquad (3)$$

$C(t)$ is the convolution output at time t, $F\,(t+b)$ represents the input at time $t+b$ and $k(b)$ is the convolution kernel or filter.

Fig. 1 illustrates the architecture of a convolutional neural.

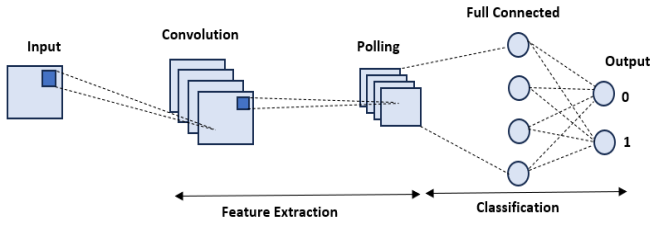

Fig.1. CNN Architecture

- Long Sort-Term Memory (LSTM): This is a special type of RNN designed to avoid the problem of long-term dependency. In this LSTM algorithm, nodes are connected to other nodes and improve learning by removing and storing specific information [16]. LSTM is used to classify attack and normal data after passing through a Dropout layer for regularization, a dense layer and a sigmoid activation function;
- CNN + LSTM: is a combination of the CNN and LSTM algorithms in a single model. This model generally consists of the Conv1D layer with an activation function commonly used in "ReLu" neural networks, followed by the LSTM layer with an "adam" optimizer. The other parameters remain the same as those used in CNN and LSTM [12].

IV. WORK METHODOLOGY

This section presents the methodology used for intrusion detection using the CNN, LSTM, CNN+LSTM, LR and NB algorithms. These algorithms are trained and tested using the CICIDS2017 dataset. In addition, they are evaluated using performance measures such as accuracy, precision, recall and f1 Score. The models will be compared with the experimental results obtained, in order to decide on the best model to be implemented in the real UAV network, and more specifically at the ground control station.

A. CICIDS2017 dataset

In this paper, we use the CICIDS2017 dataset, which is the data set collected by the Canadian Institute for Cybersecurity Research at the University of New Brunswick2 [17] over 5 days in a real network environment. The motivation for choosing CICIDS2017 is that it is considered the most practical public dataset for UAV intrusion detection, encompassing normal events as well as different types of attack. This dataset contains labeled data on various common types of attack, such as brute force, DDoS, Botnet, SQL injection, XSS, Infiltration and Heartbleed. The shape of this dataset in terms of number of records and number of features is 566486 rows and 79 columns.

This CICIDS2017 dataset is divided into two parts: 80% is allocated to algorithm training and 20% to testing.

B. Preprocessing

The CICIDS2017 dataset used in this article is in CSV format. It consists of a large number of normal and abnormal data packets. So, it's important to process this data and make it suitable for a Deep Learning method. This involves three main steps: standardization, normalization and data cleaning [18].
Several Operations are used to identify redundant features, unwanted quotes, strange characters, infinite values, categorical values and empty lines. This operation makes them usable by the algorithms during training and testing.
To detect attacks or normal traffic, in this CICIDS2017 dataset, normal traffic called 'BENIGN' is defined as '0' while attacks are considered as '1'.

C. Framework for drone network intrusion detection

The drone is made up of several components, notably the flight controller which is considered an essential part of the drone's operation, the ground control station and the communications links. However, these components are targets for cyber-attacks such as DDoS/DoS attacks, Man in The Middle, SQL injection, etc. It is possible for an intruder to gain illegal access to a system and launch these different types of attack. When an attacker gains access, he can alter data in an unauthorized way, disrupt services, intercept data, divulge confidential data, etc. One of the techniques used to deal with these intrusions is the use of an IDS.
This technique can be deployed in two ways [19]:

- Deployment of an IDS at the ground station, where all information from the UAV to the ground station is analyzed at the ground station and decisions are made on the basis of the analyzed data;
- Deployment of an IDS on the autonomous base. The IDS is integrated into the UAV control system, and the UAV acts as a host, analyzing the data and controlling other UAVs.

In this proposed framework, the model resides at the ground control station. As illustrated in the fig. 2, these UAVs represented on the architecture are independent, as they do not directly share information with each other. However, they do communicate important information (images, location information, speed, command and control data, etc.) with the base station via communications links. The intrusion detection model to be deployed at the ground control station checks and identifies all suspicious or malicious data before it is sent to the storage server. Before being transmitted to the storage server or to the drone, the data is subjected to a rigorous and thorough verification by an intrusion detection model.

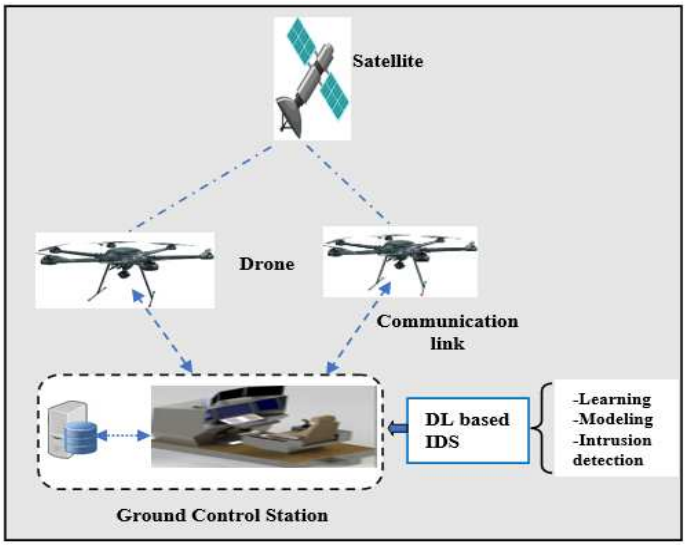

Fig.2. Intrusion detection in drones' network

The models developed in this article classify the CICIDS2017 data set received as normal or abnormal. Of this data set, 80% is used for training and 20% for testing the algorithms. If the data is identified as correct, it can be transmitted to the storage server or to the drone, but if it is identified as an attack, an alert is triggered and it is blocked.

V. TEST ENVIRONMENT AND EXPERIMENTATION

The experiment was carried out on an Intel Core i7 processor, 16 GB RAM, 1 TB hard disk. Training and testing of the algorithms were carried out in Jupyter's python environment (Sklearn), Numpy, tensorflow, etc. Considering different Machine Learning and Deep Learning algorithms such as CNN, LSTM, CNN + LSTM, LR and NB, the experiment was performed on all features. The CICIDS2017 dataset was used to train and test the algorithms, and model performance was evaluated for data classification into two classes including BENIGN defined by '0' and attacks defined by '1'. In addition, the CICIDS dataset was divided into training and test modules to evaluate the performance of the proposed models on the test data.

VI. RESULTS AND DISCUSSION

To evaluate and compare model performance, certain well-known evaluation criteria are used in research work. The parameters used to measure the performance of the models examined are accuracy, precision, recall and F1 Score. Fig. 3 compares the CNN, LSTM, CNN+LSTM, LR and NB models in terms of accuracy. Among the models considered, CNN+LSTM offers the highest accuracy score with 99.063%, followed by LSTM with 99.036%, while CNN scored 98.946%. These results show that Deep Learning models are more effective at correctly classifying data with lower error rates. In contrast, the LR model has an accuracy score of 97.466% followed by NB with a lower accuracy of 72.466%. This shows that NB is less effective in intrusion detection due to the complexity of the data using the unbalanced CICIDS2017 dataset.

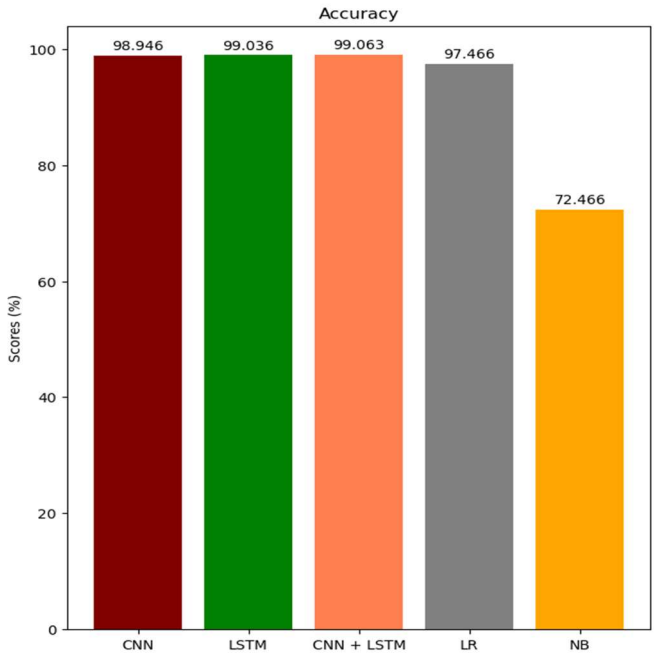

Fig.3. Accuracy of CNN, LSTM, CNN+LSTM, LR and NB

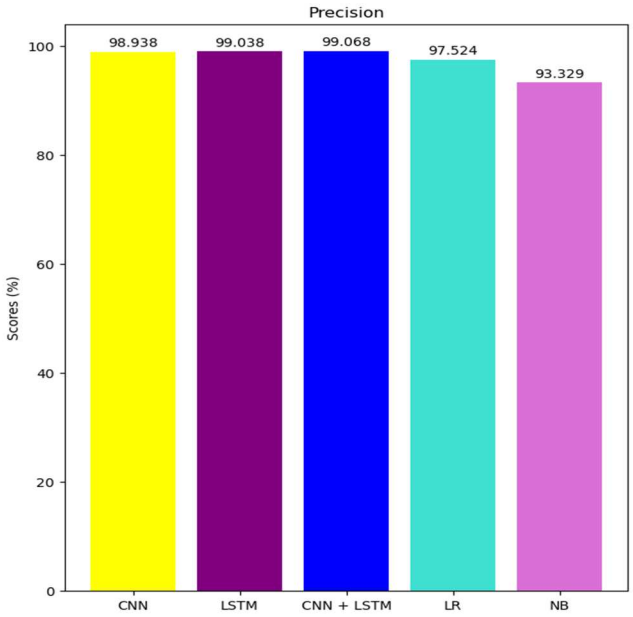

Fig.4. Precision of CNN, LSTM, CNN+LSTM, LR and NB

Fig. 4 shows a comparison of the CNN, LSTM, CNN+LSTM, LR and NB models in terms of precision.
In terms of precision, CNN+LSTM achieved a high precision of 99.068%, showing that it has a succeeded in minimizing false positives. It is followed by LSTM with 99.038%, CNN with 98.938%, LR with 97.524%. NB model shows lower precision (93.329%) compared with other models.

As shown in fig.5, CNN+LSM achieved a high recall score compared to the other models with 99.063%, showing that it is more effective at identifying attacks among all the real positive instances. The recall value of LSTM is 99.036%, CNN is 98.946%, LR is 97.466% and finally NB obtained a recall value 72.466% lower than the other models. This shows that NB fails to effectively identify real intrusions.

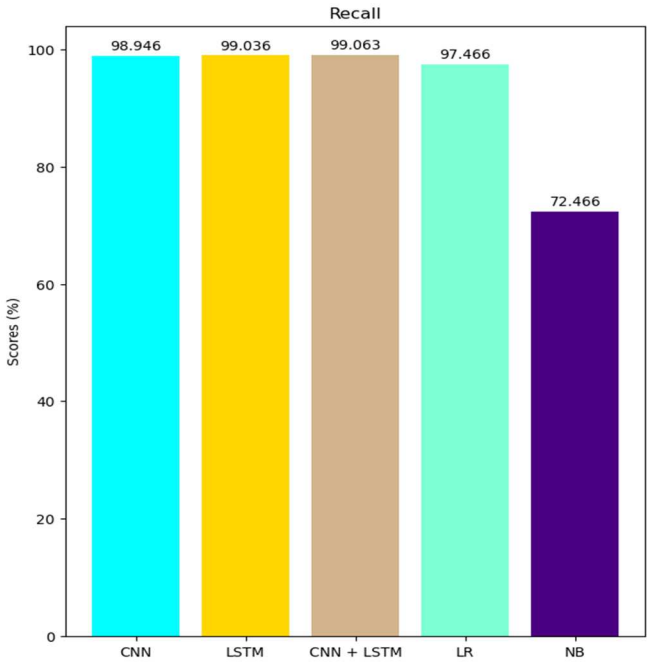

Fig.5. Recall of CNN, LSTM, CNN+LSTM, LR and NB

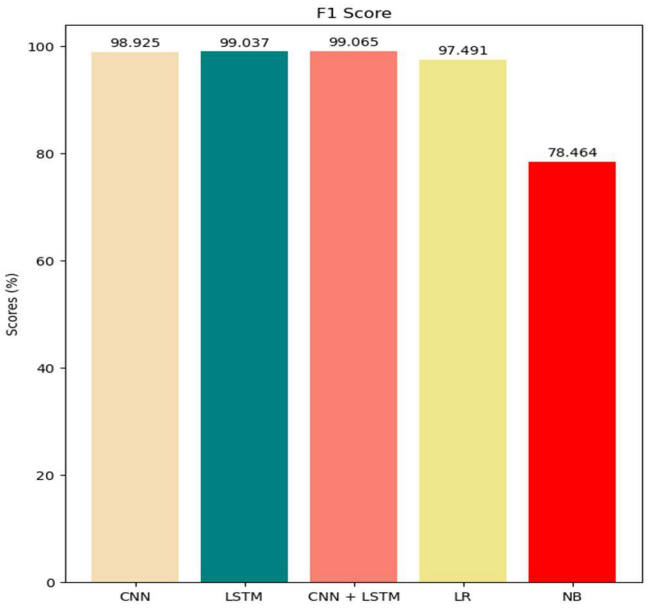

Fig.6. F1 Score of CNN, LSTM, CNN+LSTM, LR and NB

Fig. 6 also shows that the F1 Score value for CNN+LSTM (99.065%) is higher than that of the other models, showing that it is effective at detecting intrusions with a high balance between precision and recall compared with the other models examined. NB also obtained a lower score (78.464%), demonstrating its inability to adapt to complex, unbalanced data such as the CICIDS2017 dataset.

In this paper, it is important to present the Receiver Operating Characteristic (ROC). The higher the AUC, the better the model. Fig. 7 shows that CNN+LSTM is the best model for intrusion detection.

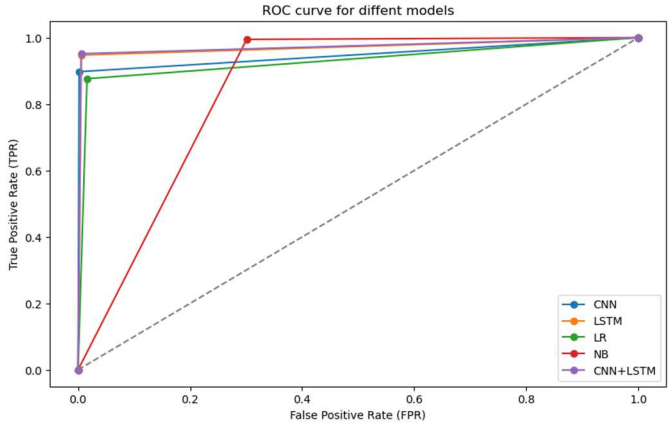

Fig.7. ROC of different Models

Table I shows the training and testing times for the different models proposed.

TABLE I. TRAINING AND TEST TIMES FOR MODELS

Models	Training Time (S)	Test Time (S)
CNN	1131.95925	32.6530
LSTM	14618.43184	185.173391
CNN+LSTM	7738.01250	107.0029
LR	301.57	0.40764
NB	4.8840	1.224

Fig.8 shows the comparison between training time and testing time of the models.

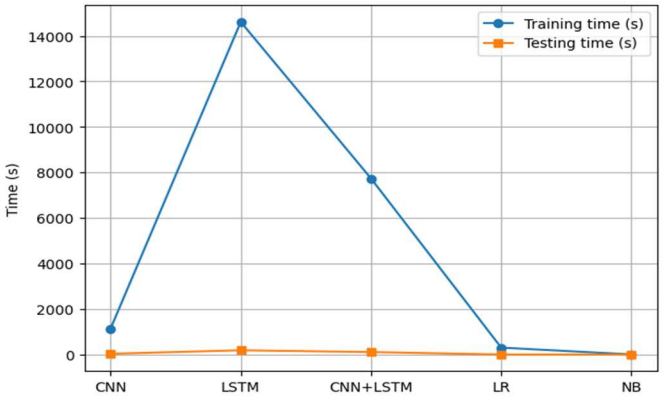

Fig.8. Training and test times for different models

Table II compares our experimental results with those of other existing works on the basis of accuracy. With regard to accuracy, our LR model showed a value 7.466% higher than that obtained in [10]. Compared with the LR model in [11], our accuracy is 9.096% higher. Compared with the CNN, LSTM and CNN+LSTM models of [12], the accuracies of our models are respectively 3.806%, 2.796% and 1.463% higher. Compared with the LR model accuracy results of [8], our LR model is superior, with a value 2.066% higher. Although [20]

obtained high accuracy results for the CNN (99.08%) and LSTM (99.37%) models, that of the CNN+LSTM model is lower (98.88%) than the results of our model (99.063%).

TABLE II. ACCURACY COMPARISON OF OUR MODELS WITH OTHER EXISTING MODELS

Ref	CNN	LSTM	CNN+LSTM	LR	NB
[10]	-	-	-	90%	-
[11]	-	-	-	88.37%	88.37%
[12]	95.14%	96.24%	97.6%	-	-
[8]	-	-	-	95.4%	-
[20]	99.08%	99.37%	98.88%	-	-
Our paper	98.946%	99.036%	99.063%	97.466%	72.5%

VII. CONCLUSION

Unmanned Aerial Vehicles are systems used in a variety of fields, such as delivery, disaster management, mapping, agriculture and more. However, UAVs cybersecurity remains a major concern. One of the cybersecurity issues in UAVs are cyberattacks that target these systems. As a result, several solutions have been developed in recent years to mitigate intrusions. In this article, we propose intrusion detection models based on Deep Learning and Machine Learning on drones. The proposed algorithms have been trained using the CICIDS2017 dataset as it is considered the public and more convenient dataset. The evaluation results indicate that CNN+LSTM is able to detect intrusions using the CICIDS2017 dataset with a high accuracy of 99.063% and a lower error rate of 0.00937.

Finally, based on comparison with other models considered, we find that the results obtained outperform those of existing intrusion detection models. In our future work, we intend to implement the hybrid CNN+LSTM model, which performed better in a real drone network environment, as explained in Section IV.

REFERENCES

[1] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends," *Intell. Serv. Robot.*, vol. 16, no. 1, pp. 109–137, 2023, doi: 10.1007/s11370-022-00452-4.

[2] C. Guerber, M. Royer, and N. Larrieu, "Machine Learning and Software Defined Network to secure communications in a swarm of drones," *J. Inf. Secur. Appl.*, vol. 61, 2021, doi: 10.1016/j.jisa.2021.102940.

[3] M. Cosar, "Cyber attacks on unmanned aerial vehicles and cyber security measures," *Eurasia Proc. Sci. Technol. Eng. Math.*, vol. 21, pp. 258–265, 2022, doi: 10.55549/epstem.1226251.

[4] S. N. Ashraf *et al.*, "IoT empowered smart cybersecurity framework for intrusion detection in internet of drones," *Sci. Rep.*, vol. 13, no. 1, pp. 1–20, 2023, doi: 10.1038/s41598-023-45065-8.

[5] L. Alzubaidi *et al.*, *Review of deep learning: concepts, CNN architectures, challenges, applications, future directions*, vol. 8, no. 1. Springer International Publishing, 2021. doi: 10.1186/s40537-021-00444-8.

[6] A. M. Abdulghani, M. M. Abdulghani, W. L. Walters, and K. H. Abed, "Improving Intrusion Detection in UAV Communication Using an LSTM-SMOTE Classification Method," *J. Cyber Secur.*, vol. 4, no. 4, pp. 287–298, 2022, doi: 10.32604/jcs.2023.042486.

[7] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-learning-enabled intrusion detection system for cellular connected uav networks," *Electron.*, vol. 10, no. 13, pp. 1–28, 2021, doi: 10.3390/electronics10131549.

[8] A. Shrivastava and K. Sharma, "DDoS Detection for Amateur Internet of Flying Things using Machine Learnings," *SSRN Electron. J.*, no. Aece, pp. 124–133, 2022, doi: 10.2139/ssrn.4159111.

[9] S. Ouiazzane, F. Barramou, and M. Addou, "Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 351–362, 2020, doi: 10.14569/IJACSA.2020.0111044.

[10] R. A. Ramadan, A. H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," *Electron.*, vol. 10, no. 21, 2021, doi: 10.3390/electronics10212633.

[11] Z. Baig, N. Syed, and N. Mohammad, "Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning," *Futur. Internet*, vol. 14, no. 7, pp. 1–20, 2022, doi: 10.3390/fi14070205.

[12] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.

[13] O. Simeone, "A Very Brief Introduction to Machine Learning with Applications to Communication Systems," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 4, pp. 648–664, 2018, doi: 10.1109/TCCN.2018.2881442.

[14] Y. Kesenek, I. Özçelik, and E. Kaya, "A new document classification algorithm against malicious data leakage attacks," *J. Fac. Eng. Archit. Gazi Univ.*, vol. 37, no. 3, pp. 1639–1654, 2022, doi: 10.17341/gazimmfd.641580.

[15] A. S. A. Issa and Z. Albayrak, "DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM," *Acta Polytech. Hungarica*, vol. 20, no. 2, pp. 105–123, 2023, doi: 10.12700/APH.20.2.2023.2.6.

[16] R. Yao, N. Wang, Z. Liu, P. Chen, and X. Sheng, "Intrusion detection system in the advanced metering infrastructure: A cross-layer feature-fusion CNN-LSTM-based approach," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–17, 2021, doi: 10.3390/s21020626.

[17] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems," *Int. J. Eng. Technol.*, vol. 7, no. 3.24 Special Issue 24, pp. 479–482, 2018.

[18] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[19] G. Choudhary, V. Sharma, I. You, K. Yim, I. R. Chen, and J. H. Cho, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," *2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018*, pp. 560–565, 2018, doi: 10.1109/IWCMC.2018.8450305.

[20] A. Samy, H. Yu, and H. Zhang, "Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning," *IEEE Access*, vol. 8, pp. 74571–74585, 2020, doi: 10.1109/ACCESS.2020.2988854.