Received: 9 April 2025 | Revised: 30 July 2025 | Accepted: 10 August 2025 | Published online: 9 October 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2026, Vol. 5(1) 44–52
DOI: 10.47852/bonviewJCCE52025886

BON VIEW PUBLISHING

Comparative Analysis of ML-Based Intrusion Detection System for Cyber-Physical UAV System

Hafiz Muhammad Attaullah[1,2], Muhammad Harris[2], Inam Ullah Khan[1], Muhammad Mansoor Alam[1,3] and Mazliham Mohd Su'ud[1,*]

[1] *Faculty of Computing and Informatics, Multimedia University, Malaysia*

[2] *Faculty of Computing, Mohammad Ali Jinnah University, Pakistan*

[3] *Faculty of Computing, Riphah International University, Pakistan*

Abstract: Unmanned Aerial Vehicles (UAV) represent a new generation of intelligent solutions that improve productivity and safety in agriculture, security, and healthcare services. However, they are more prone to cyber-attacks such as data manipulation, spoofing, vague attacks, and false data injection due to increasing integration of Cyber-Physical Systems. This research proposes an anomaly-based intrusion detection system (IDS) for UAVs with real-time cognition of cyberspace and physical presence using Machine Learning (ML) algorithms to achieve strong performance metrics. The feature set includes both cyber-object characteristics (such as network traffic and IP addresses) and physical-object characteristics (such as sensor data), collected under both normal and adversarial conditions. This data is used to train and evaluate the proposed approach. Prior to training, exploratory data analysis, normalization, and data balancing using the Synthetic Minority Oversampling Technique (SMOTE) were performed to maximize the efficiency of the feature space. A well-known cyber-physical dataset, T_ITS, was used in this process. The results show that high-quality preprocessing significantly improves key performance metrics such as accuracy, precision, recall, and F1-score. Among the classifiers, Extreme Gradient Boosting (XGBoost) and Light Gradient Boosting Machine (LightGBM) were identified as the top performers achieving an accuracy of 99.18%. These results emphasize the importance of robust IDS frameworks in securing UAV operations against rising threat of cyber-attacks.

Keywords: UAV safety, anomaly detection, IDS, cyber-physical systems, cybersecurity threats, feature engineering

1. Introduction

Unmanned Aerial Vehicles (UAV) or drones are rapidly being transformed by their innovative capabilities across many industries. Almost every sector now depends almost entirely on autonomous machines that fly without human pilots on board, entirely revolutionizing safety and efficiency [1]. UAVs replace human presence in dangerous environments when human presence is avoidable or unacceptable. To enable effective control of these operations for real time monitoring and guiding drones to operate smoothly, dedicated control centers are created. Over the years, with automation, artificial intelligence, sensor technology advancement, and UAVs are increasingly performing more automated and more reliable tasks, taking on the responsibility that once required very careful manual intervention. UAVs are extremely useful in every field such as agriculture, environment monitoring, security, aerial photography, transport, construction, and healthcare today. However, they are adaptable (can take many problems on their own) which results in increased safety and efficiency. For instance, drones are used to monitor crop health, soil condition data, and data work to help promote precision farming for maximum productivity and minimum resource consumption at least in agriculture [2, 3]. During security incidents, using UAVs enable continuous monitoring and better situational awareness compared to traditional security methods and surveillance applications. One can envision the evolution of drones: starting as large and heavy machines, gradually getting smaller and more efficient, until a small Lindbergh-style drone capable of righting itself mid-air and performing tasks like picking up trash in urban areas or along rivers (the first of the flying Roombas) . At the same time, these advancements have expanded the operational range of UAVs, making many systems increasingly reliant on them [4, 5]. However, UAVs are subjected to major challenges, particularly in cybersecurity. Cyber and physical threats including data hijacking, spoofing, false data injection (FDI), electromagnetic pulse (EMP) attacks, and brute force password breaches put UAV operations at risk. The safety, reliability, and efficiency of UAV systems rely on tackling these problems [6–11].

***Corresponding author:** Mazliham Mohd Su'ud, Faculty of Computing and Informatics, Multimedia University, Malaysia. Email: mazliham@mmu.edu.my

2. Related Work

This section presents a comprehensive review of the literature on Machine Learning (ML) based intrusion detection systems. It examines key methodologies from previous research and analyzes their contributions to the field.

Jonsson and Olovsson [12] conducted a review of 62 studies published between 2014 and 2024 in primary databases, following the PRISMA model guidelines and categorizing IDS based on detection methods, algorithms, datasets, types of attacks, and software environments. It identifies some of the main problems in references by Arafah et al. [13], Prokhorenkova et al. [14], Nazir et al. [15], Diro and Chilamkurti [16], Alrawais et al. [17], Ahanger et al. [18], and

Abdallah et al. [19], including the large number of false positives, resource constraints, and the unavailability of standard datasets and presents some emerging trends and future directions of research on how UAV can be made more secure. A study by Yoo et al. [20] investigates ML-based anomaly detection within the context of Aviation CPS. The authors emphasize that unsupervised learning is a promising approach, particularly due to the limited availability of labeled aviation data. In addition, they point to the emergence of hybrid models that potentially increase detection accuracy and robustness. Some of the most important issues mentioned in a study by Heydarian et al. [21] are the inaccessibility of publicly available datasets and evaluation measures, other than just accuracy, limiting its future developments to containing standardized datasets, a better hybrid method, and inclusion of explainable AI (XAI) approach in enhancing model interpretability [22].

Aamir and Zaidi [23] proposed a decentralized learning framework in intrusion detection of CPS. Their work is concerned with using Federated learning in a scenario where feeding the data to the centralized models has the drawbacks of data-sharing, with the addition of differential privacy because of its advantages in enhancing data safety. Deng et al. [24] and Macrina et al. [25] take this topic by contrasting the centralized and decentralized models, and conclude that despite having a better detection performance, centralized models are associated with a higher risk of privacy. Kim et al. [26] understand the structures of privacy-preserving IDs that would adopt the ability to classify network traffic with a high degree of accuracy used by the CPS forcing organizational sensitive information to be nullified.

In references [27–36], essential security and privacy needs, the assessment of the threats, and the countermeasures that might be used to address those threats were discussed and identified. These researches are highly concentrated on IDSs by using machine learning in the context of UAVs, including what techniques should be used in terms of detection, features they select, test datasets, and the metrics of the algorithm's performance. Besides evaluating the benefits and weaknesses of the existing UAV IDSs, they also determine research gaps and propose future improvements to the UAV cybersecurity [37, 38].

3. Intrusion Detection System for UAV

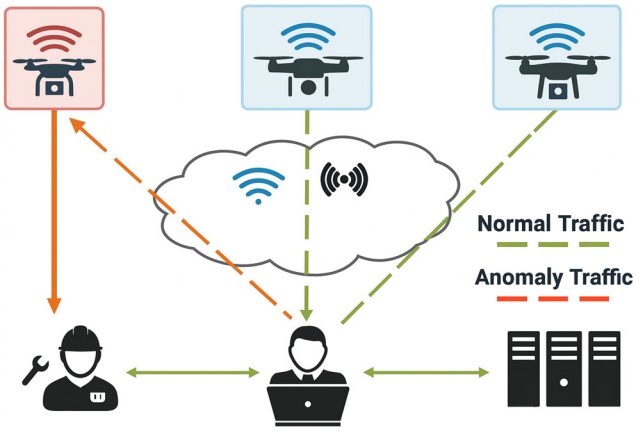
IDS can be broadly classified into three categories:

1) Signature-Based IDS, which relies on predefined attack patterns and signatures to detect known threats but is ineffective against zero-day attacks.
2) Anomaly-Based IDS, which employs machine learning and statistical models to identify deviations from normal behavior, enabling the detection of novel and previously unseen threats; and
3) Hybrid IDS, which combines both signature-based and anomaly-based techniques to improve detection accuracy and adaptability.

UAV network anomalies are effectively detected through anomaly-based IDS because this solution can analyze both cyber (network traffic, authentication logs, IP addresses) and physical (sensor readings, GPS coordinates, altitude, velocity) parameters [39–42].

Anomaly based IDS for UAVs uses ML and statistical methods (SMs) to analyze UAV suspicious activities activities/behaviors and decides if these behaviors are anomalous on a real-time basis. IDS is more important in detecting new threats that previous pattern-based systems such as signature-based systems (SBS) cannot discern. In real time of the network traffic and unmanned aerial vehicles operation, the anomaly-based IDS improves the security of UAVs in the context of the cyber-attacks and systems' failures. Figure 1 presents a detailed view of components in the UAV anomaly detection system [43]. To better ensure the safety of UAVs, ML methods or algorithms have been introduced into the research of UAV safety such as, Support

Figure 1
Anomaly based intrusion detection system for UAV



Vector Machine (SVM), Extreme Gradient Boosting (XGBoost), HistGradientBoostingClassifier (HGBC), K-Nearest Neighbors Classifier (KNC), and Light Gradient Boosting Machine (LightGBM), which enhance detection accuracy and reduce possible false alarms.

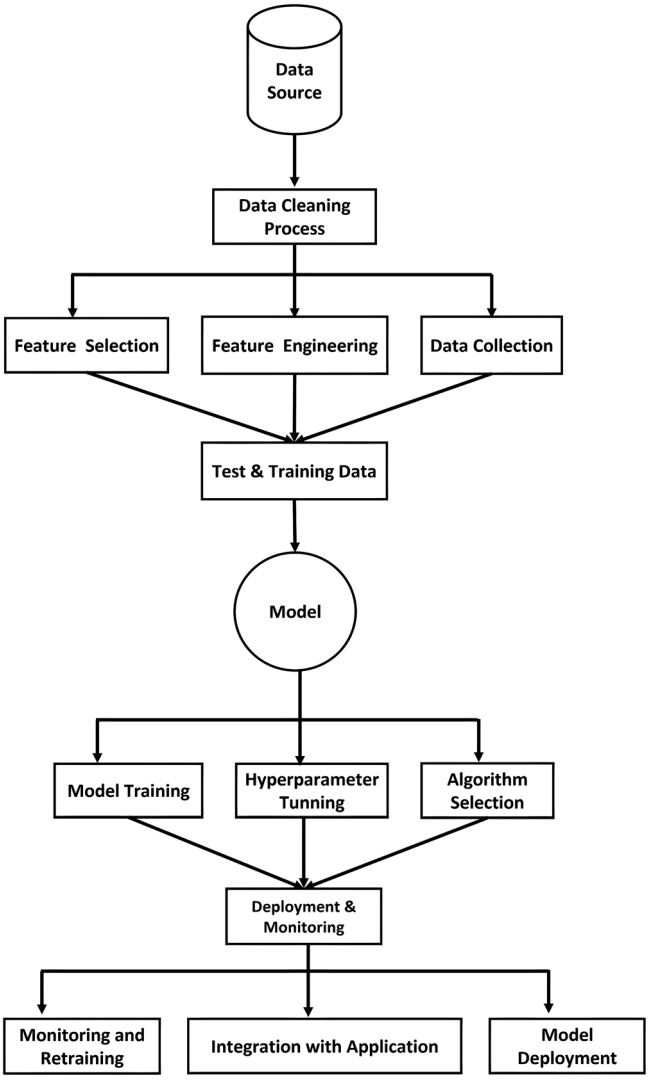
4. Methodology

In addition to refining, we need to think about better training of ML algorithms; high content of accurate data is crucial to gain better outcomes. Normally, they are produced by hardware subsystems and are kept in files or in a database. However, in our dataset [1, 43] raw data at this state is not utilizable for ML training in its basic format. It should not only be preprocessed but also be refined to create a training dataset. This process includes several steps: the issues of missing values, scaling through standardization, converting categorical data into numerical through label encoding, and normalization. Finally, the dataset is divided into training and testing zones. These steps help allow the ML classifier to do well in training and to be evaluated well on this test set. During the simulation process, data was collected in two phases [44]. The initial part consisted of training flights where no cybersecurity threats were implemented while the second part included five distinct forms of cyber threats. The packets of WiFi traffic generated in the Tello drone network were secured using the airodump-ng tool, which captures the network traffic. A fixed flight plan was used, mimicking operations such as farming or surveillance, and the drone transferred sensor data to the control unit in 0.5 seconds per intervals. Parameters measured roll, pitch, yaw rates, speed, and temperatures of motors. During flight, the drone was programmed to carry out random tasks at 10%, 20%, and 50% chance of it executing the action such as moving and flipping by left or right. In total, 35 flights were conducted: twenty normal flights, where no cyber-attack was performed, and fifteen flights with different cyber-attack scenarios. The collected data was categorized into physical data (obtained from the sensors of the drone) and cyber data (file format: packet capture (PCAP)). This dataset was utilized to analyze the performance of the drone in normal and cyber-attack scenarios. The data includes five categories: such as Distributed Denial-of-Service (DDoS) Attack, Benign Attack, Evil Twin Attack, FDI Attack, and Replay Attack. From the analysis of these attacks, it will be possible to determine the potential of IDS for UAVs. IDS models can identify and notify UAVs about the occurrence of a cyber-attack and possibly out of usual behavior to improve the security and dependability of UAV systems by mitigating the risk of cyber threats [45–52]. In Table 1, the classification of attacks presented in the T_ITS dataset is described [1]. Below are the different cyber-attacks.

Table 1
Comparative analysis of ML-based IDS research findings

Study/reference	Key focus	Identified limitations
[12]	AIDS	High false positive rates, lack of standard datasets, resource constraints
[13–19]	SIDS	Same as above – false positives, resource usage, dataset limitations
[20]	AIDS	Few labeled datasets, difficulty in applying supervised learning, need for hybrid/ unsupervised models
[21, 22]	AIDS	Lack of public datasets, overreliance on accuracy metric, missing explainability (XAI)
[23]	AIDS	Centralized models risk privacy; need for decentralized and privacy-preserving approaches
[24, 25]	DIDS	Trade-off between performance and privacy; centralized systems perform better but are less secure
[26]	PIDS	Sensitive organizational data risk, limited adoption of high-accuracy private models
[27–36]	ML-IDS	Dataset issues, vague threat models, unclear feature selection, inconsistent metrics across evaluations
[37, 38]	AIDS	Lack of standardized approaches; need for improvement in detection models and performance metrics

Figure 2
Proposed workflow



The dataset structure was cleaned and restructured to allow for analysis and training of a model. First, columns with numeric data were identified, and initial replacements of invalid values (i.e., text or special characters) from those columns with Not a Number (NaN) were performed. We then substituted out these NaN with 0s for consistency. To prevent all future errors and to ensure the class-based analysis is done only when it should be, rows with missing values on critical class columns were dropped. They transformed categorical columns to the category data type as categorical columns take up more memory and transformed time stamp columns to numeric values so that we can-do time-based pattern analysis [53–55]. Columns that did not introduce any errors were dropped to simplify the dataset. To convert categorical variables into a machine learning compatible form, we applied Label Encoding [56–59]. Furthermore, the SMOTE synthesized new data points for the minority class to address the class imbalance. This was a very important step to avoid hydrangea models being biased toward the most dominant class and at the same time reduce hydrangea risks from overfitting the data to make it realistic. By looking into the preprocessing steps done to this dataset, we ensured that it is all clean and ready for efficient and reliable ML tasks by following the cleaning and training ML as proposed in the methodology in Figure 2.

5. Results

The evaluation of ML models was conducted using the T_ITS dataset in order to assess their classification performance. The most crucial factors for classification appear in both the feature importance chart and the confusion matrices for model accuracy displays. The bar chart along with the table demonstrates that XGBoost (99.08%) coupled with CatBoost Classifier (CBC) (99.18%) reaches the top performance achievable because these models yield exceptional accuracy measures together with precise outcomes and superior recall and F1-score measurements.

Various networks can generate a large volume of traffic in the IDS, and therefore its feature engineering and selection are indispensable for creating efficient machine learning. Feature selection is the process of selecting, purging or deriving respective features from raw data, which excludes noisy or useless data. Thus, IDS increases the threat detection coefficients due to concentration on those aspects that are the most important, otherwise the abundance of information only generates confusion. Targeted feature selection also reduces computation cost and makes it easier to interpret the model at the end of the day. The flaw becomes critical while selecting features and other attributes that are involved include the false alarm rate. This is a case of having more ‘false

positives,' or where an alert system identifies non-threatening activities as a problem when in fact they are not, and false 'negatives,' where a real problem is overlooked by the system [60]. That kind of trade-off directly affects IDS and shows the need for constant optimization of a feature set.

Data cleaning and preprocessing encompass essential steps performed prior to data analysis and modeling. It is the first and a foundational step when developing and constructing sound ML models. This entails steps like data cleaning, data reduction where one removes noise, data condensation where one must delete undesired information, and data integration where one integrates many datasets. Preprocessing is important since the input data of high quality enhances the reliability of the models together with predictive performance [61–64]. Performing this step will lead to incorrect predictions as well as skewness in the output data, which in turn will lead to an erroneous propagation of the issues affecting the usability of the model. After the refining, testing multiple datasets lets researchers compare the strength of models that have been developed. In the end, the results of the experiment showed that cleaned and filtered datasets improve classifier accuracy as the quality of the input data affects the entire learning process.

In the context of feature importance evaluation, it is very critical to know which attributes influence model significantly. For instance, a bar graph in Figure 3 with the distribution of feature importance demonstrated that "timestamp_c" and "time_last_packet" are the most significant carriers, taking up to 32.06% and 27.20, respectively. These time-related metrics therefore strongly indicate that their use is very relevant, especially in the measurement of network patterns. Other important characteristics are identified as "wlan.seq" at 8.97%, "wlan. duration" at 6.05%, "ip.id" at 4.62%, data.data at 4.43%, and wlan.ra at 4.30%, proving wireless and IP data's impact. On the other hand, there was no impact presented by some features including "tcp. dsport," "wlan.sa," "tcp. flags," and "tcp. window_size" with an importance of 0%. Whenever such insignificant characteristics are detected and eliminated within a model, the resulting improved efficiency contributes to decreased costs for calculations and more straightforward interpretations of results while maintaining the level of accuracy.

Following data preprocessing, several machine learning classifiers were used to classify the attacks on the T_ITS dataset. To compare the classifiers, means of performance measures including precision, recall, and F1-score were employed. The results showed that all classifiers were quite successful, and that measures of precision and recall were equivalent. Several algorithms, including XGBoost Classifier, CatBoost Classifier, and LightGBM Classifier, demonstrated superior performance in comparative evaluations. The results suggest that the dataset was well preprocessed and the models well-tuned. The comparison of these classifiers is presented in Figure 4 and Table 2, where the number of the classifiers was considered in the above list; the accuracy, precision, recall, and F1-score values are presented in the table. Taken together, all these results demonstrated the positive effects of clean and optimized raw data on algorithm performance. The enhancement shown on the classifiers is commensurate on the need for data preprocessing in improving the models for predictive analytics.

A comparative analysis of the classifiers' performance using three key metrics was conducted: We report precision, recall, and F1-score which provide clues about how each classifier works. Moreover, Figure 4 indicates that all the algorithms performed well over the T_ITS dataset, having a better balance between precision, recall, and F1 score metrics.

To further assess classifier performance, we estimated the distribution of true and false predictions for each model. As shown in Figure 5, tree-based classifiers such as XGBoost, CatBoost, and Random Forest Classifier produced a high number of true positives and true negatives, with significantly lower false positives and false negatives. In contrast, SVM exhibited a comparatively higher rate of misclassification, particularly in the form of false positives. These results reinforce the advantage of ensemble methods in reducing detection errors in IDS system. Also, Figure 6 illustrates the Receiver Operating Characteristic (ROC) curves for all classifiers in this environment. Each curve depicts the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR), with the Area Under the Curve (AUC) providing a single-value summary of classification performance.

Figure 3
Dataset T_ITS feature importance

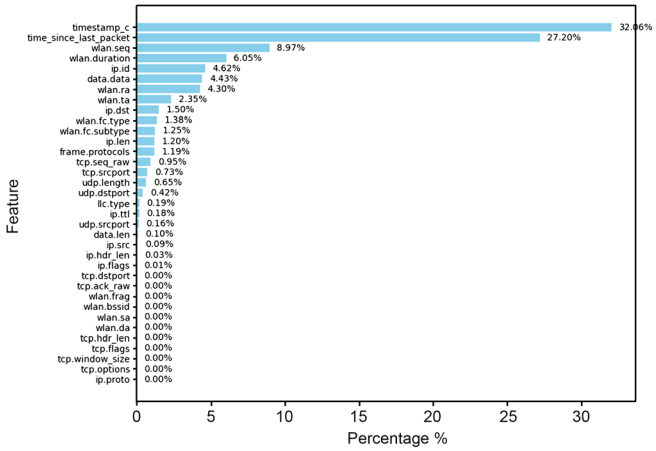


Figure 4
Performance metrics for algorithms

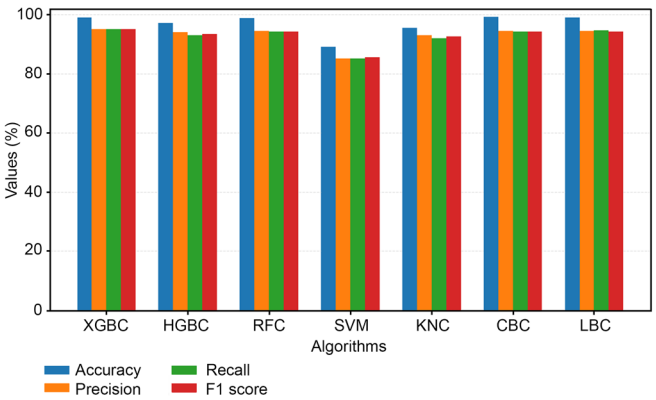


Table 2
Distribution of different types of cyber-attacks in T_ITS dataset

Attack type	Attack type	Environment	Start index	End index
Benign	–	Cyber	1	9426
		Physical	9427	13,717
DoS attack	Active	Cyber	13,718	25,389
		Physical	25,390	26,363
Replay attack	Active	Cyber	26,364	38,370
		Physical	38,371	39,344
Evil twin	Active	Cyber	39,345	45,028
		Physical	45,029	50,502
FDI	Active	Cyber	50,503	53,976
		Physical	53,977	54,784

Figure 5
True positives, true negatives, false positives, and false negatives for each classifier on the T_ITS dataset

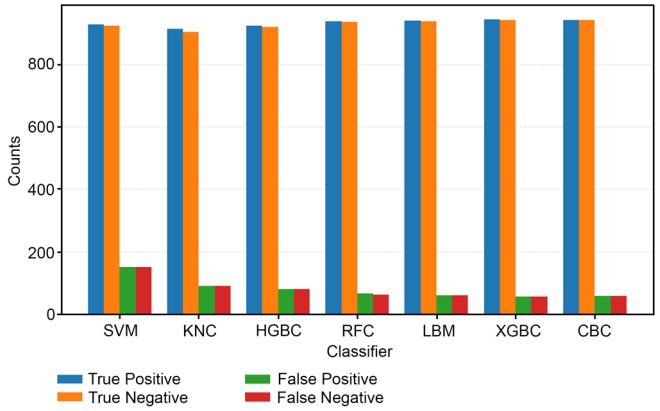
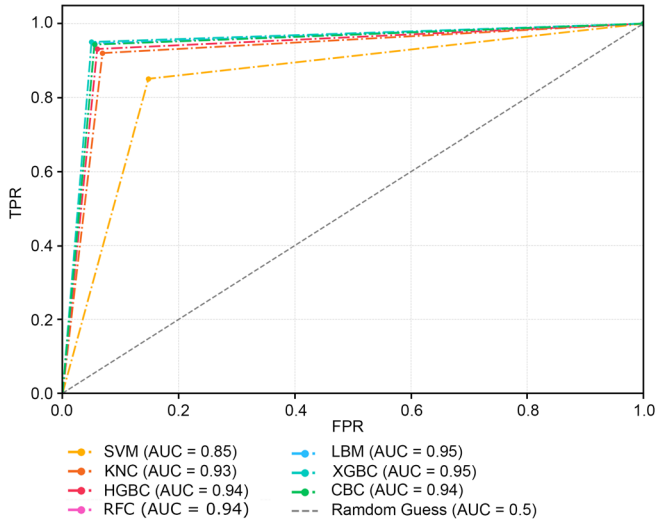


Figure 6
ROC curves for all classifiers evaluated on the T_ITS dataset



Among the models, XGBoost and LightGBM achieved the highest AUC scores (0.95), indicating strong discriminatory power. CatBoost and Random Forest Classifier followed closely, demonstrating reliable detection capabilities. In contrast, SVM exhibited the lowest AUC (0.85), suggesting relatively weaker performance in distinguishing between attack and benign instances. Overall, the ROC curves affirm the effectiveness of tree-based ensemble models for this network.

Table 3 illustrates dramatic improvement in algorithm performance especially with XGBC and CBC when clean and filtered data is used. Figures 7–13 present heatmaps for top classifiers, which represent the performance assessment results of classification techniques used for HGBC and KNN, SVM and XGBoost, and LightGBM and RNF Machine Learning models. The network analysis models use a classification system to identify data points such as Denial-of-Service (DoS) attacks, Replay attacks, Benign operations, or an unknown category. The results in the confusion matrices show that both XGBoost and RNF and HGBC correctly classified 2310 DoS attacks together with 2358 Replay attacks and 1882 Benign instances and presented low error rates.

The trained LightGBM model performed outstandingly by correctly identifying 1881 Benign instances, 2369 Replay attack instances, and 2307 DoS attack instances. On the other hand, SVM demonstrated misclassification failure that involved classifying 428

Table 3
Results of various classifiers' accuracy score using T_ITS dataset

T_ITS dataset using following classifier	Accuracy score	Precision score	Recall score	F-1 score
SVM	89.02	85.21	85.06	85.47
KNC	95.42	93.12	92.02	92.5
HGBC	97.17	94.03	93.12	93.5
RFC	98.91	94.5	94.35	94.25
LBM	99.03	94.5	94.65	94.25
XGBC	99.08	95.01	95.03	95.15
CBC	99.18	94.5	94.34	94.25

Figure 7
Confusion matrix heatmap (CatBoost model)

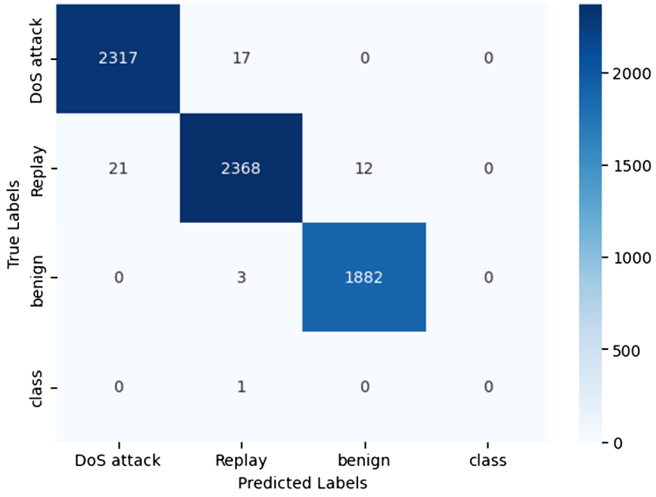
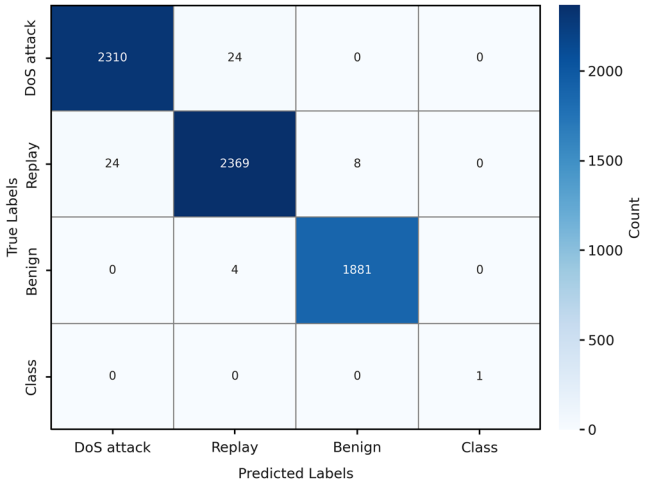


Figure 8
Confusion matrix heatmap (XGBoost model)



DoS attack samples and mistyping 155 Replay attack samples, thus decreasing accuracy rates. An evaluation of KNN model classification indicates that the system faces two major limitations since it misinterprets 100 Replay attacks and 62 benign instances as Replay attacks demonstrating its weaknesses when analyzing intricate network traffic patterns.

Figure 9
Confusion matrix heatmap (LightGBM model)

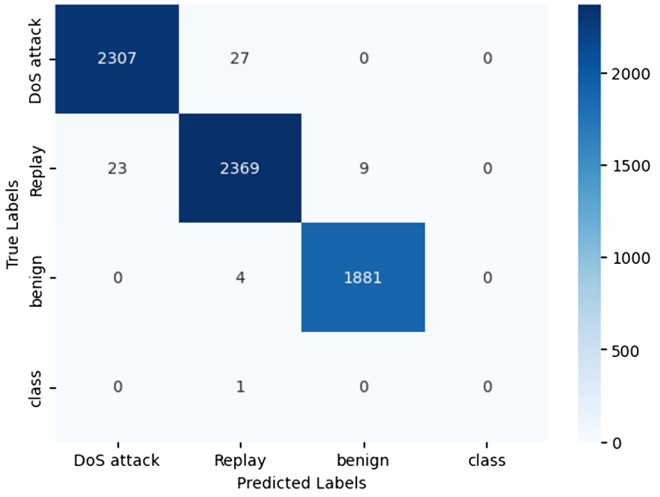


Figure 10
Confusion matrix heatmap (RNF model)

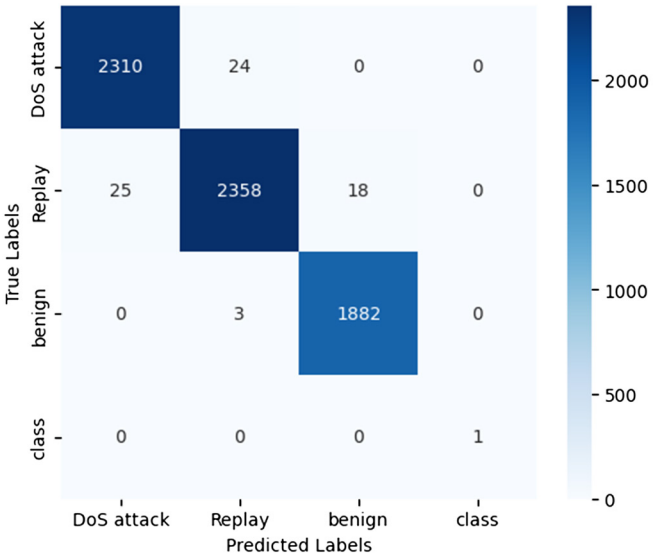


Figure 11
Confusion matrix heatmap (HGBC model)

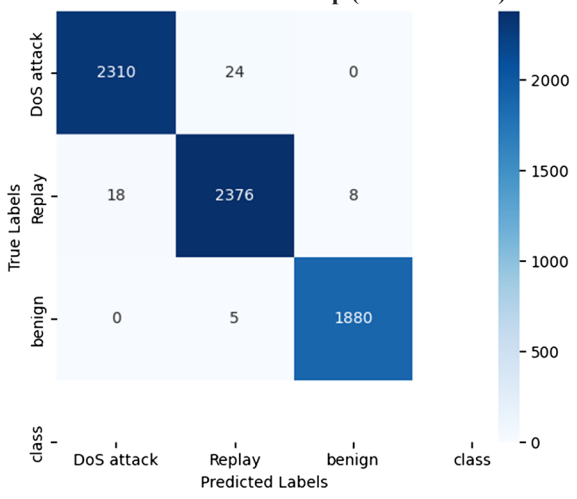


Figure 12
Confusion matrix heatmap (KNN model)

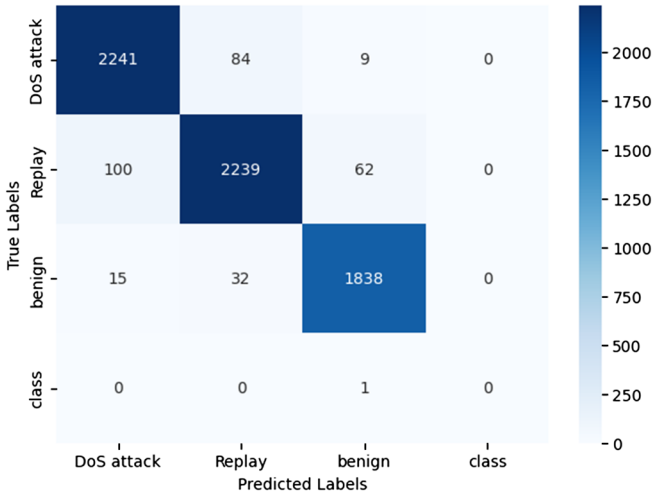


Figure 13
Confusion matrix heatmap (SVM model)

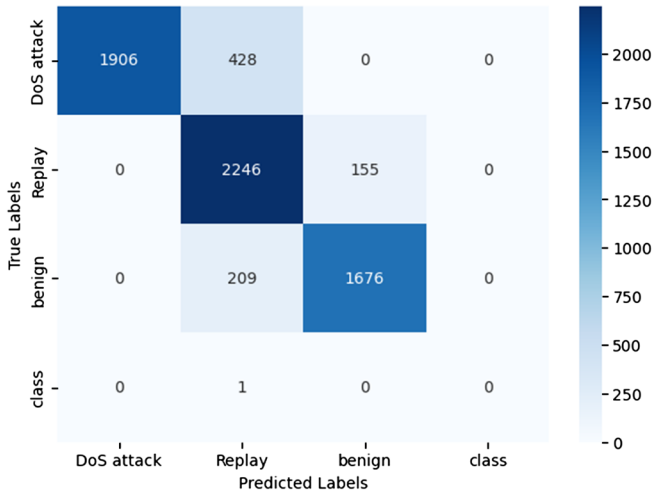


Table 4
Mean performance scores and standard deviation across 5-fold stratified cross-validation

Metric	Mean	Standard deviation
Accuracy	79.10%	± 2.82%
F1-score	78.33%	± 2.83%
AUC	93.40%	± 0.93%

Finally, we applied a 5-fold stratified cross-validation to validate the model's generalization performance. As a result, Table 4 represents the average performance of our best classifier that demonstrates a consistent accuracy of 79.10% and macro F1-score of 78.33%, which indicates a balanced classification across potentially imbalanced class distributions. The high AUC score (93.40%) suggests strong discriminative capability, meaning the classifier is effective at distinguishing between attack types and benign traffic. The low standard deviations across all metrics confirm that the model performs stably across different folds, reducing concerns about data split bias or overfitting.

6. Conclusion

UAVs have completely changed the way things are done in fields like agriculture, security, healthcare, and military operations. These drones have become more efficient and versatile with advancements in automation, AI, and the technologies of their sensor package. Despite these, challenges such as poor battery life, lack of mobility, and inherent vulnerability to Benign, Replay, FDI, and DoS attacks continue to persist. In order to handle these, we focused on a dataset and cleaned and prepared it (removing duplicates, removing missing values by imputation, filtering outliers, and encoding categorical values using label encoding and string conversion). Secondly, we balanced out data distribution across classes with sampling and filtration approaches for feature engineering, categorical encoding, and Transformation for better dataset usability. After making necessary checks and data cleaning, we tested the algorithms like XGBC, HGBC, RFC, SVM, KNC, CBC, and LGBM to determine which performed best. We evaluated the models with metrics such as the confusion matrix, accuracy, precision, recall, F1 score, and heatmaps to get some insight about their performance. As we approach the future, more sensible integration of more intelligent IDS systems such as advanced deep learning models, graph algorithms, and metaheuristic techniques are promising to further increase the efficiency and security of UAVs. These new capabilities will meet growing data demands, respond to emerging cyber threats, and allow UAVs to continue to transform the industry while protecting operations.

Acknowledgment

The authors are grateful to MMU and TM Malaysia for the support.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support the findings of this study are openly available at https://doi.org/10.1109/TITS.2023.3339728, reference number [1]. The data that support the findings of this study are openly available at https://dx.doi.org/10.21227/6f22-py65, reference number [43].

Author Contribution Statement

Hafiz Muhammad Attaullah: Conceptualization, Methodology, Software, Resources, Data curation, Writing – original draft, Writing – review & editing. **Muhammad Harris:** Conceptualization, Methodology, Software, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Inam Ullah Khan:** Methodology, Resources, Data curation, Writing – review & editing, Visualization. **Muhammad Mansoor Alam:** Validation, Formal analysis, Investigation, Resources, Data curation, Writing – review & editing, Project administration. **Mazliham Mohd Su'ud:** Validation, Formal analysis, Investigation, Resources, Data curation, Writing – review & editing, Supervision, Project administration.

References

[1] Hassler, S. C., Mughal, U. A., & Ismail, M. (2024). Cyber-physical intrusion detection system for unmanned aerial vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(6), 6106–6117. https://doi.org/10.1109/TITS.2023.3339728

[2] Yang, T., Chen, J., Deng, H., & Lu, Y. (2023). UAV abnormal state detection model based on timestamp slice and multi-separable CNN. *Electronics*, *12*(6), 1299. https://doi.org/10.3390/electronics12061299

[3] Vaughn, R. B., Sira, A., & Dampier, D. A. (2002). Information security system rating and ranking. *The Journal of Defense Software Engineering*, *15*(5), 30–32.

[4] Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

[5] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133

[6] Choi, S. Y., & Cha, D. (2019). Unmanned aerial vehicles using machine learning for autonomous flight; state-of-the-art. *Advanced Robotics*, *33*(6), 265-277. https://doi.org/10.1080/01691864.2019.1586760

[7] Louvieris, P., Clewley, N., & Liu, X. (2013). Effects-based feature identification for network intrusion detection. *Neurocomputing*, *121*, 265–273. https://doi.org/10.1016/j.neucom.2013.04.038

[8] Blázquez-García, A., Conde, A., Mori, U., & Lozano, J. A. (2021). A review on outlier/anomaly detection in time series data. *ACM Computing Surveys*, *54*(3), 56. https://doi.org/10.1145/3444690

[9] Cook, A. A., Mısırlı, G., & Fan, Z. (2020). Anomaly detection for IoT time-series data: A survey. *IEEE Internet of Things Journal*, *7*(7), 6481–6494. https://doi.org/10.1109/JIOT.2019.2958185

[10] Gopalakrishna, R., & Spafford, E. H. (2005). *A trend analysis of vulnerabilities*. Purdue University. https://www.cerias.purdue.edu/bookshelf/archive/2005-05.pdf

[11] Choi, K., Yi, J., Park, C., & Yoon, S. (2021). Deep learning for anomaly detection in time-series data: Review, analysis, and guidelines. *IEEE Access*, *9*, 120043–120065. https://doi.org/10.1109/ACCESS.2021.3107975

[12] Jonsson, E., & Olovsson, T. (1997). A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, *23*(4), 235–245. https://doi.org/10.1109/32.588541

[13] Arafah, M., Phillips, I., Adnane, A., Hadi, W., Alauthman, M., & Al-Banna, A.-K. (2025). Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks. *Applied Soft Computing*, *168*, 112455. https://doi.org/10.1016/j.asoc.2024.112455

[14] Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V., & Gulin, A. (2018). CatBoost: Unbiased boosting with categorical features. In *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, 6639–6649.

[15] Nazir, A., Memon, Z., Sadiq, T., Rahman, H., & Khan, I. U. (2023). A novel feature-selection algorithm in IoT networks for intrusion detection. *Sensors*, *23*(19), 8153. https://doi.org/10.3390/s23198153

[16] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761-768. https://doi.org/10.1016/j.future.2017.08.043

[17] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34–42. https://doi.org/10.1109/MIC.2017.37

[18] Ahanger, A. S., Khan, S. M., & Masoodi, F. (2021). An effective intrusion detection system using supervised machine learning techniques. In *2021 5th International Conference on Computing Methodologies and Communication*, 1639–1644. https://doi.org/10.1109/ICCMC51019.2021.9418291

[19] Abdallah, E. E., Wafa' Eleisah, & Otoom, A. F. (2022). Intrusion detection systems using supervised machine learning techniques: A survey. *Procedia Computer Science*, *201*, 205-212. https://doi.org/10.1016/j.procs.2022.03.029

[20] Yoo, W., Yu, E., & Jung, J. (2018). Drone delivery: Factors affecting the public's attitude and intention to adopt. *Telematics and Informatics*, *35*(6), 1687-1700. https://doi.org/10.1016/j.tele.2018.04.014

[21] Heydarian, M., Doyle, T. E., & Samavi, R. (2022). MLCM: Multi-label confusion matrix. *IEEE Access*, *10*, 19083–19095. https://doi.org/10.1109/ACCESS.2022.3151048

[22] Uddin, M. F., Lee, J., Rizvi, S., & Hamada, S. (2018). Proposing enhanced feature engineering and a selection model for machine learning processes. *Applied Sciences*, *8*(4), 646. https://doi.org/10.3390/app8040646

[23] Aamir, M., & Zaidi, S. M. A. (2019). DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *International Journal of Information Security*, *18*(6), 761–785. https://doi.org/10.1007/s10207-019-00434-1

[24] Deng, X., Liu, Q., Deng, Y., & Mahadevan, S. (2016). An improved method to construct basic probability assignment based on the confusion matrix for classification problem. *Information Sciences*, *340–341*, 250-261. https://doi.org/10.1016/j.ins.2016.01.033

[25] Macrina, G., di Puglia Pugliese, L., Guerriero, F., & Laporte, G. (2020). Drone-aided routing: A literature review. *Transportation Research Part C: Emerging Technologies*, *120*, 102762. https://doi.org/10.1016/j.trc.2020.102762

[26] Kim, J., Kim, S., Jeong, J., Kim, H., Park, J.-S., & Kim, T. (2019). CBDN: Cloud-based drone navigation for efficient battery charging in drone networks. *IEEE Transactions on Intelligent Transportation Systems*, *20*(11), 4174–4191. https://doi.org/10.1109/TITS.2018.2883058

[27] Zhang, S., Zhang, H., Di, B., & Song, L. (2019). Cellular UAV-to-X communications: Design and optimization for multi-UAV networks. *IEEE Transactions on Wireless Communications*, *18*(2), 1346–1359. https://doi.org/10.1109/TWC.2019.2892131

[28] Kuhn, M., & Johnson, K. (2019). *Feature engineering and selection: A practical approach for predictive models*. USA: CRC Press. https://doi.org/10.1201/9781315108230

[29] Mohsan, S. A. H., Khan, M. A., Noor, F., Ullah, I., & Alsharif, M. H. (2022). Towards the unmanned aerial vehicles (UAVs): A comprehensive review. *Drones*, *6*(6), 147. https://doi.org/10.3390/drones6060147

[30] Chen, H., Wang, Z., Yang, S., Luo, X., He, D., & Chan, S. (2025). Intrusion detection using synaptic intelligent convolutional neural networks for dynamic Internet of Things environments. *Alexandria Engineering Journal*, *111*, 78–91. https://doi.org/10.1016/j.aej.2024.10.014

[31] Ibrahim, A. A., Ridwan, R. L., Muhammed, M. M., Abdulaziz, R. O., & Saheed, G. A. (2020). Comparison of the CatBoost classifier with other machine learning methods. *International Journal of Advanced Computer Science and Applications*, *11*(11), 738–748. https://doi.org/10.14569/IJACSA.2020.0111190

[32] Ucgun, H., Yuzgec, U., & Bayilmis, C. (2021). A review on applications of rotary-wing unmanned aerial vehicle charging stations. *International Journal of Advanced Robotic Systems*, *18*(3), 17298814211015863. https://doi.org/10.1177/17298814211015863

[33] Dong, F., Li, L., Lu, Z., Pan, Q., & Zheng, W. (2019). Energy-efficiency for fixed-wing UAV-enabled data collection and forwarding. In *2019 IEEE International Conference on Communications Workshops*, 1–6. https://doi.org/10.1109/ICCW.2019.8757098

[34] Elmeseiry, N., Alshaer, N., & Ismail, T. (2021). A detailed survey and future directions of unmanned aerial vehicles (UAVs) with potential applications. *Aerospace*, *8*(12), 363. https://doi.org/10.3390/aerospace8120363

[35] Mallidi, S. K. R., & Ramisetty, R. R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. *Discover Internet of Things*, *5*(1), 8. https://doi.org/10.1007/s43926-025-00099-4

[36] Diana, L., Dini, P., & Paolini, D. (2025). Overview on intrusion detection systems for computers networking security. *Computers*, *14*(3), 87. https://doi.org/10.3390/computers14030087

[37] Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E. H. M., Shahzad, T., & Khan, M. A. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Scientific Reports*, *15*(1), 1726. https://doi.org/10.1038/s41598-025-85866-7

[38] Osmani, K., & Schulz, D. (2024). Comprehensive investigation of unmanned aerial vehicles (UAVs): An in-depth analysis of avionics systems. *Sensors*, *24*(10), 3064. https://doi.org/10.3390/s24103064

[39] Jacob, S. L., & Habibullah, P. S. (2025). A systematic analysis and review on intrusion detection systems using machine learning and deep learning algorithms. *Journal of Computational and Cognitive Engineering*, *4*(2), 108–120. https://doi.org/10.47852/bonviewJCCE42023249

[40] Walling, S., & Lodh, S. (2025). An extensive review of machine learning and deep learning techniques on network intrusion detection for IoT. *Transactions on Emerging Telecommunications Technologies*, *36*(2), e70064. https://doi.org/10.1002/ett.70064

[41] Al-Haija, Q. A., & Droos, A. (2025). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*, *42*(2), e13726. https://doi.org/10.1111/exsy.13726

[42] Hui, B., & Chiew, K. L. (2025). An improved network intrusion detection method based on CNN-LSTM-SA. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *44*(1), 225–238. https://doi.org/10.37934/araset.44.1.225238

[43] Hassler, S., Mughal, U., & Ismail, M. (2023). *Cyber-physical dataset for UAVs under normal operations and cyber-attacks* [Data set]. IEEE Dataport. https://doi.org/10.21227/6f22-py65

[44] Ruseno, N., & Lin, C.-Y. (2025). Real-time UAV trajectory prediction for UTM surveillance using machine learning. *Unmanned Systems*, *13*(02), 505-519. https://doi.org/10.1142/S230138502550030X

[45] Nasir, Z. U. I., Iqbal, A., & Qureshi, H. K. (2024). Securing cyber-physical systems: A decentralized framework for collaborative intrusion detection with privacy preservation. *IEEE Transactions on Industrial Cyber-Physical Systems*, *2*, 303–311. https://doi.org/10.1109/TICPS.2024.3425794

[46] Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Scientific Reports*, *15*(1), 4617. https://doi.org/10.1038/s41598-025-87028-1

[47] Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Machine learning-based intrusion detection systems for the Internet of Drones: A systematic literature review. *IEEE Access*, *13*, 96681–96714. https://doi.org/10.1109/ACCESS.2025.3575236

[48] AL-Syouf, R. A., Bani-Hani, R. M., & AL-Jarrah, O. Y. (2024). Machine learning approaches to intrusion detection in unmanned aerial vehicles (UAVs). *Neural Computing and Applications*, *36*(29), 18009–18041. https://doi.org/10.1007/s00521-024-10306-y

[49] Eshmawi, A. A., Umer, M., Ashraf, I., & Park, Y. (2024). Enhanced machine learning ensemble approach for securing small unmanned aerial vehicles from GPS spoofing attacks. *IEEE Access*, *12*, 27344–27355. https://doi.org/10.1109/ACCESS.2024.3359700

[50] Rajathi, C., & Rukmani, P. (2025). Hybrid Learning Model for intrusion detection system: A combination of parametric and non-parametric classifiers. *Alexandria Engineering Journal*, *112*, 384–396. https://doi.org/10.1016/j.aej.2024.10.101

[51] Tahir, M., Abdullah, A., Udzir, N. I., & Kasmiran, K. A. (2025). A novel approach for handling missing data to enhance network intrusion detection system. *Cyber Security and Applications*, *3*, 100063. https://doi.org/10.1016/j.csa.2024.100063

[52] Agnew, D., del Aguila, A., & McNair, J. (2024). Enhanced network metric prediction for machine learning-based cyber security of a software-defined UAV relay network. *IEEE Access*, *12*, 54202–54219. https://doi.org/10.1109/ACCESS.2024.3387728

[53] Tiwari, P. K., Prakash, S., Tripathi, A., Yang, T., Rathore, R. S., Aggarwal, M., & Shukla, N. K. (2025). A secure and robust machine learning model for intrusion detection in Internet of Vehicles. *IEEE Access*, *13*, 20678–20690. https://doi.org/10.1109/ACCESS.2025.3532716

[54] Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, *22*(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

[55] Ahmed, M. A. O., Abdelsatar, Y., Alotaibi, R., & Reyad, O. (2025). Enhancing Internet of Things security using performance gradient boosting for network intrusion detection systems. *Alexandria Engineering Journal*, *116*, 472–482. https://doi.org/10.1016/j.aej.2024.12.106

[56] Yu, H., Zhang, W., Kang, C., & Xue, Y. (2025). A feature selection algorithm for intrusion detection system based on the enhanced heuristic optimizer. *Expert Systems with Applications*, *265*, 125860. https://doi.org/10.1016/j.eswa.2024.125860

[57] Wisanwanichthan, T., & Thammawichai, M. (2025). A lightweight intrusion detection system for IoT and UAV using deep neural networks with knowledge distillation. *Computers*, *14*(7), 291. https://doi.org/10.3390/computers14070291

[58] Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). Deep learning-driven methods for network-based intrusion detection systems: A systematic review. *ICT Express*, *11*(1), 181–215. https://doi.org/10.1016/j.icte.2025.01.005

[59] Yan, Y., Yi, D., Lu, H., & Gao, L. (2025). Control and applications of intelligent unmanned aerial vehicles. *Electronics*, *14*(2), 375. https://doi.org/10.3390/electronics14020375

[60] Jain, M., & Srihari, A. (2025). Comparison of machine learning algorithm in intrusion detection systems: A review using binary logistic regression. *Authorea International Journal of Computer Science and Mobile Computing*, *13*(10), 45–53. https://doi.org/10.22541/au.174837862.20090642/v1

[61] Zhou, W., Xia, C., Wang, T., Liang, X., Lin, W., Li, X., & Zhang, S. (2025). HIDIM: A novel framework of network intrusion detection for hierarchical dependency and class imbalance. *Computers & Security*, *148*, 104155. https://doi.org/10.1016/j.cose.2024.104155

[62] Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. *International Journal of Information Security*, *24*(1), 3. https://doi.org/10.1007/s10207-024-00921-0

[63] Fares, H., Zeroual, M., Karim, A., Maleh, Y., Baddi, Y., & Aknin, N. (2025). Machine learning, deep learning and ensemble learning based approaches for intrusion detection enhancement. *EDPACS*, *70*(1), 31–51. https://doi.org/10.1080/07366981.2024.2422645

[64] Bacha, A. M., Zamoum, R. B., & Lachekhab, F. (2025). Machine learning paradigms for UAV path planning: Review and challenges. *Journal of Robotics and Control*, *6*(1), 215–233. https://doi.org/10.18196/jrc.v6i1.24097

How to Cite: Attaullah, H. M., Harris, M., Khan, I. U., Alam, M. M., & Su'ud, M. M. (2026). Comparative Analysis of ML-Based Intrusion Detection System for Cyber-Physical UAV System. *Journal of Computational and Cognitive Engineering*, *5*(1), 44–52. https://doi.org/10.47852/bonviewJCCE52025886