ML-based Intrusion Detection for Drone IoT Security

Abdullah Al-Fuwaiers [1], Shailendra Mishra [2]
[1] Department of Information Technology College of Computer and Information Sciences,Majmaah University, Majmaah, Saudi Arabia
[2] Department of Information Technology College of Computer and Information Sciences,Majmaah University, Majmaah, Saudi Arabia
Emails: 441104422@s.mu.edu.sa; s.mishra@mu.edu.sa

Abstract

The integration of drones into various industries brings about cybersecurity challenges due to their reliance on internet connectivity. To address this, we propose a comprehensive cybersecurity architecture leveraging machine learning (ML) algorithms and Internet of Things (IoT) technologies within the Internet of Drones (IoD) framework. Our architecture employs IoT-enabled sensors strategically placed across the drone ecosystem to collect and analyze data on system behaviors, communication patterns, and environmental variables. This data is then processed by a centralized platform equipped with sophisticated ML algorithms for pattern identification and anomaly detection. A key feature is the dynamic learning mechanism, enabling real-time intrusion detection by adapting to evolving threats. By combining IoT and ML, the system proactively defends against cyberattacks by distinguishing between typical and abnormal activity. Emphasis is placed on data integrity and confidentiality through secure communication protocols and cryptographic algorithms. Extensive simulations and tests validate the framework's effectiveness in various IoD scenarios, demonstrating its ability to swiftly identify intrusions and informing future enhancements. This comprehensive study meticulously examines the pressing cybersecurity concerns within the burgeoning drone industry. It proposes a robust architectural framework designed to enhance security for drone-enabled applications in our increasingly interconnected world. By harnessing the synergies between Internet of Things (IoT) and Machine Learning (ML) technologies, this innovative approach aims to fortify the integrity and reliability of drone systems.

Keywords: Cyber security; IoT; Drone; neural networks; IDS; machine learning

1. Introduction

The proliferation of drones in various industries has led to the emergence of the Internet of Drones (IoD), where drones are interconnected through wireless networks to perform collaborative tasks efficiently [1]. However, the integration of drones into IoT ecosystems brings forth new cybersecurity challenges, as these aerial vehicles become susceptible to malicious attacks and unauthorized access. Ensuring the security and integrity of drone networks is paramount to safeguarding sensitive data, protecting privacy, and maintaining operational continuity.The convergence of Internet of Things (IoT) and drone technologies holds immense promise, ushering in a new era of possibilities [2]. This amalgamation, however, is not without its challenges, particularly in the realm of cybersecurity [3]. The vulnerabilities inherent in this integration necessitate a comprehensive and forward-thinking approach to secure the communication channels and ensure the data integrity of interconnected drones. Traditional security measures designed for more conventional networks may fall short in addressing the intricacies of this dynamic and distributed system.

Drones are rapidly evolving from standalone devices to integral components within IoT ecosystems. This paradigm shift brings forth a pressing need for an advanced cybersecurity framework that

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

strategically leverages the unique capabilities of IoT technologies. As drones become increasingly integrated into various sectors, from agriculture and surveillance to logistics and emergency response, the stakes for securing these systems have never been higher.

The aim of this study is to develop an effective intrusion detection system (IDS) for the Internet of Drones (IoD) utilizing machine learning (ML) techniques. The primary objectives include:

1. Designing and implementing a robust IoT-enabled cybersecurity framework tailored specifically for drone networks.
2. Investigating and selecting suitable ML algorithms for intrusion detection, considering the unique characteristics and constraints of drone-based IoT environments.
3. Training and fine-tuning the selected ML models using labeled datasets to accurately detect and classify anomalous behavior and potential security threats.
4. Providing insights into the practical challenges and considerations involved in deploying and managing cybersecurity solutions for IoD, along with recommendations for enhancing security resilience.

This research contributes to the advancement of cybersecurity in the realm of drone-based IoT by:

- Introducing a novel approach to intrusion detection utilizing machine learning algorithms tailored for the specific requirements of drone networks.
- Providing a comprehensive evaluation of the proposed IDS system's performance under various conditions, thereby offering valuable insights for both academia and industry practitioners.
- Addressing the growing concerns regarding the security and privacy implications of integrating drones into IoT ecosystems, thus fostering safer and more secure deployment of drone technologies in diverse applications.

Through this work, we aim to bolster the security posture of Internet-connected drones and facilitate their widespread adoption across domains while mitigating potential cybersecurity risks.

2. Related Work

The integration of drones into the Internet of Things (IoT) has prompted a surge of research addressing the complex interplay between unmanned aerial vehicles and cybersecurity. Existing studies have shed light on the conventional security measures employed in IoT-enabled drone systems, emphasizing encryption, authentication, and intrusion detection systems. However, these efforts often fall short in accommodating the decentralized architecture of drone networks and the dynamic nature of their communication patterns. Some notable contributions have explored the application of machine learning techniques for anomaly detection in drone networks. Addressing IoT cybersecurity challenges for government applications, [4] stresses the urgency of research, policy development, and systematic approaches to tackle security concerns. Additionally, research [5] explores architectural issues impacting drone network security, advocating for secure Internet of Drones (IoD) frameworks. Integration of IoT in healthcare systems, as discussed in [6], enhances services but exposes vulnerabilities in data transmission, necessitating robust security measures.

Furthermore, frameworks utilizing metaheuristic techniques for intelligent cyber threat detection [7], and focusing on cyber-physical satellite and aerial vehicle systems security [8], are proposed. Studies [9] and [10] highlight the growing attention towards Unmanned Aerial Vehicles (UAVs) and propose logistic regression as an approach for security attack estimation in IoT-based UAV networks. Lastly, a classification process employing Deep Belief Networks (DBN) and Sparrow Search Optimization (SSO) algorithm is presented in [11]. These studies collectively contribute to advancing understanding and strategies for addressing security challenges across various technological landscapes.While machine learning shows promise in enhancing security, a critical gap remains in the literature concerning the development of a specialized cybersecurity framework exclusively tailored for the Internet of Drones. This [12] research aims to address this gap by proposing a novel framework that leverages machine learning for adaptive intrusion detection and behavioral analysis, providing a more dynamic and responsive approach to securing IoT-enabled drone systems.

By emphasizing a comprehensive and specialized approach, this research [13] seeks to advance the current state of knowledge in IoT security for unmanned aerial vehicles.[14] proposes a system using

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

deep learning and machine learning techniques for effective detection, with promising evaluation metrics.The prevalence of supervised, unsupervised, and semi-supervised learning in addressing cyber threats, citing examples in communication networks, IoT networks, and cloud computing. [15] highlights the limited research on ML applications in drone network security, introducing an access control mechanism as a novel contribution in the context of drone cybersecurity, distinguishing itself from previous works such as [16], a blockchain-based solution that lacked suitability for IoT-based drone networks. The authors [17] devised a novel two-stage model, integrating LSTM and Random Forest, for efficient attack flow detection in network traffic, introduced an LSTM Autoencoder for precise identification of individual attacks with minimal features, analyzed an SVM model for short-duration attack flow detection, and openly shared a low-rate attack dataset on GitHub.

2.1 Research Gaps and Challenges:

Detecting intrusions in the Internet of Drones (IoD) is a complex challenge that demands a sophisticated cybersecurity framework, particularly in the context of the rapidly evolving threat landscape and the interconnected nature of drones within the IoT ecosystem [18]. While IoT technologies provide a wealth of sensor data from drones, the current state of cybersecurity lacks a holistic solution that seamlessly integrates this data with machine learning (ML) algorithms specifically designed for drone security [19]. The research focus should emphasize the development of a dynamic defense mechanism that not only enhances detection accuracy but also enables proactive responses to emerging threats, ultimately ensuring the integrity and security of internet-connected drones [20]. This integration of IoT and ML technologies represents a pivotal step towards a comprehensive cybersecurity solution for the IoD, addressing the current gap and providing a foundation for future advancements in drone security.

3. Research Methodology

The research design of the Unmanned Aerial Vehicle (UAV) framework employs a combination of machine learning (ML) and deep learning (DL) approaches for intrusion detection (IoD) within UAV networks. Specifically designed to cater to the network structure where drones establish connections with base and ground stations for transaction management, the framework comprises two essential components: the base station and the ground station, both entrusted with the responsibility of capturing and processing data.

Unlike conventional networks with centralized modules, the envisioned drone framework necessitates distinct hybrid modules for the base and ground stations. The base station module manages all drone communications, validating the drone's module selection. Distributed modules are utilized for detecting and evaluating the level and nature of attacks. Each drone is equipped with a module dedicated to monitoring attacks directly, while a second module is positioned at the ground base station. These modules collaborate to validate attacks and determine which drones warrant notification.

All drones in the airspace can communicate with the base station, a singular station, or a network of stations. The choice between streaming or batching for drone intrusion detection hinges on the technology utilized. Batch processing becomes essential when employing MapReduce as a significant decision-making component, requiring development time. Conversely, runtime identification can be achieved through frameworks such as Flink, Storm, Apache Kafka, or Spark. In this research, Apache Kafka is favoured for its efficient handling of massive data streams, especially in the initial stages.

The study emulates real-time analysis by streaming data to the modules. The layered architecture of drone attacks within the smart framework is illustrated in figure 1 . The framework primarily consists of two components: drones and base stations. The proposed model introduces a hierarchical structure with distinct layers designed to facilitate efficient operation within the context of industrial drones. At the drone layer, camera-equipped quadcopters serve as the initial tier, collecting IoT sensor data through smart sensors like GPS, radar, and altitude sensors. An unmanned aircraft system (UAS) oversees flight operations and sensor data logging, communicating with the ground controller through a specially designed communication link. The edge processing layer is responsible for data verification, transmission, and communication, utilizing an Azure IoT gateway for cloud connectivity

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

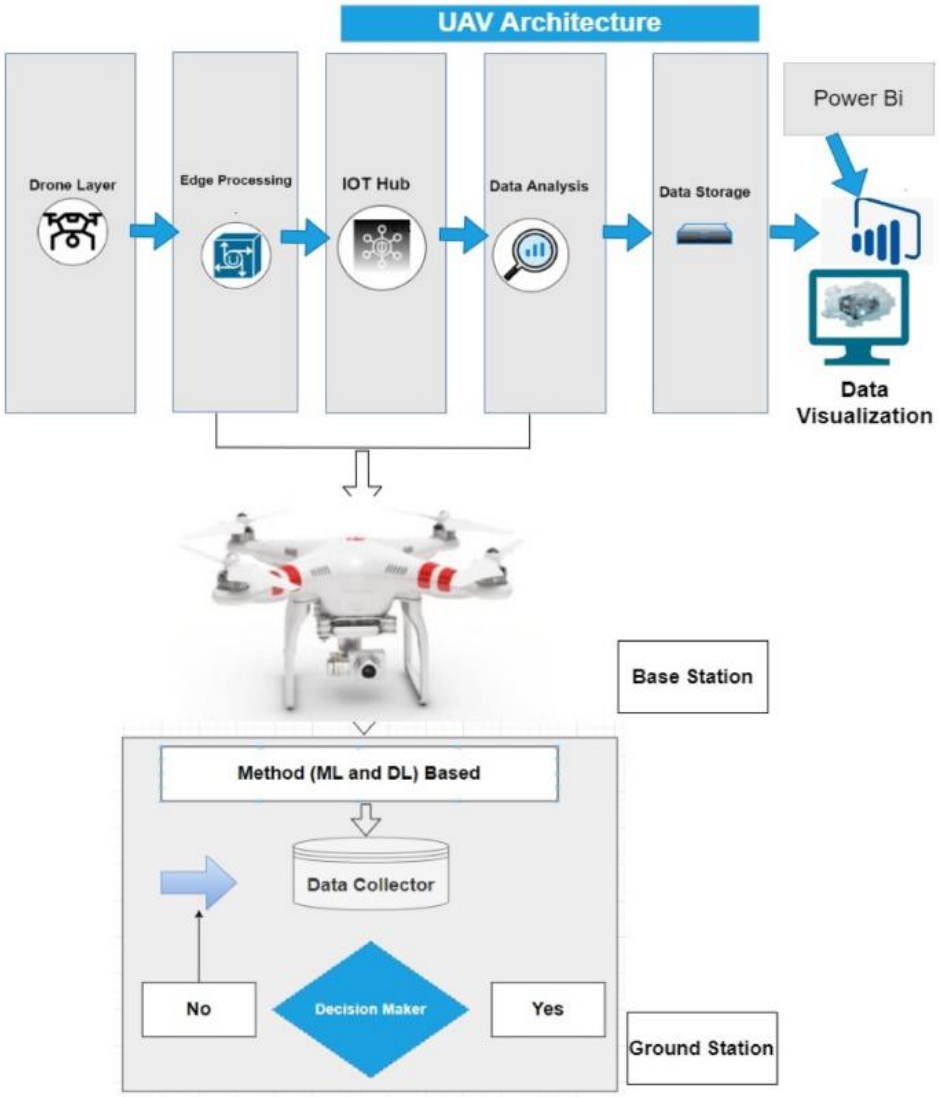

Figure 1: Research framework

This layer plays a crucial role in managing data flow, ensuring quick information transfer through Wi-Fi connectivity. The subsequent security and privacy layer employ machine learning models for device authentication and access control, addressing potential threats to physical, behavioral, and location privacy. Authentication procedures combat security concerns like spoofing and intrusion attacks. The device connection layer facilitates connectivity through IoT gateways, ensuring secure connections to the cloud-based IoT hub for authenticated devices. A security orchestration and automation module further enhances device connectivity and real-time security through blockchain technology, ensuring data integrity and protection on a cloud server. This hierarchical structure ensures a comprehensive and secure framework for the Internet of Drones (IoD), with considerations for data privacy, device authentication, and secure communication.

The integration of IoT sensors, data collection, and machine learning (ML) for subsequent data analysis involves a multi-step process. First, IoT sensors are selected and deployed on drones or in the drone environment to capture relevant data. This data is then transmitted to a server or centralized cloud for further processing. Before analysis, the raw data undergoes preprocessing to clean and organize it, addressing missing numbers, eliminating noise, and formatting the data for ML algorithms.

Machine learning algorithms are then trained using historical data to recognize patterns, correlations, and anomalies linked to typical and invasive drone behavior. Real-time data collection allows IoT sensors to continually gather data from drones during operating scenarios, feeding the ML model with up-to-date knowledge. The trained ML model is used to analyze incoming data in real-time, identifying abnormalities or departures from typical drone behavior. Alerts are generated in the event

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

of intrusions or unusual drone activity, ensuring prompt reactions to security risks. In-depth data analysis is performed on the outcomes produced by the ML model, assessing intrusion detection accuracy, observing trends in security occurrences, and enhancing the overall security posture. Continuous improvement mechanisms are implemented for the ML model, involving periodic retraining with new data to enhance accuracy and adaptability to evolving drone behaviors and threats.

A feedback loop is established between the ML model and IoT sensors, where insights gained from data analysis inform adjustments to sensor configurations, improving the overall effectiveness of the IoT-enabled smart cybersecurity framework. This end-to-end process seamlessly integrates IoT sensor data collection with machine learning for advanced analysis, enabling the development of a dynamic and adaptive cybersecurity solution for the Internet of Drones.

3.1 Machine learning Algorithms

KNN predicts the target variable of a given data point by assessing the majority class or average value among its k nearest neighbors in the feature space. The algorithm relies on a distance metric, typically Euclidean, to quantify the similarity between data points, although alternative metrics such as Manhattan or Minkowski can be utilized. The decision rule hinges on the majority class for classification tasks.Naïve Bayes belongs to generative learning algorithms, modeling input distribution for a given class. This approach, founded on the assumption of conditional independence of features given the class, facilitates quick and accurate predictions in statistical.

Random Forest is a popular supervised learning algorithm used for both classification and regression tasks. It employs the ensemble learning technique, which involves using multiple classifiers to solve complex problems and improve model performance. In Random Forest, the algorithm constructs an ensemble of decision trees, each trained on different subsets of the dataset. By combining the predictions from these trees and using the majority vote, Random Forest enhances predictive accuracy compared to using a single decision tree.

LSTMs incorporate key components such as memory cells, forget gates, input gates, and output gates, allowing them to maintain long-term memory, control information flow, and capture dependencies over extended sequences. Widely applied in natural language processing, time series prediction, speech recognition, and healthcare, LSTMs excel in tasks requiring the understanding of contextual information and long-range dependencies. Their versatility, ability to handle sequential data, and effective training mechanisms have made LSTMs a go-to choice in various domains, despite considerations of computational complexity and the need for careful hyperparameter tuning.

3.2 Dataset

In the context of intrusion detection systems (IDS), the NSL-KDD dataset plays a pivotal role. It serves as a benchmark for contemporary IDS, offering a comprehensive and representative collection of internet traffic data. As an enhancement of the KDD'99 dataset, NSL-KDD provides a more refined and realistic representation of existing networks. Its significance lies in its ability to simulate and assess the efficacy of intrusion detection mechanisms, thereby contributing to the development and evaluation of robust cybersecurity solutions in the face of evolving threats in modern-day internet traffic.

3.3 Metric Evaluations

In evaluating the effectiveness of intrusion detection systems (IDS) within drone networks, key performance metrics such as accuracy, precision, recall, and F1 score play a pivotal role.

- $Accuracy=\frac{TP+TN}{TP+TN+FP+FN}$Accuracy=TP+TN+FP+FNTP+TN
- $Precision=\frac{TP}{TP+FP}$Precision=TP+FPTP
- $Recall=\frac{TP}{TP+FN}$Recall=TP+FNTP
- $F1\ Score=2\times\frac{Precision\times Recall}{Precision+Recall}$F1 Score=Precision+Recall2×Precision ×Recall

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

4. Implementation and Experiment Analysis

In the experimental analysis of this study a comprehensive exploratory data analysis eda was conducted on the nsl kdd dataset the primary aim of the EDA was to gain insights into the inherent characteristics of the dataset assess its distribution and identify any patterns or anomalies descriptive statistics data visualizations and statistical measures were employed to explore the dataset s features understand its structure and uncover potential trends related to intrusion detection. In the exploratory data analysis eda phase a thorough examination of the dataset including descriptive statistics and visualizations was conducted to uncover patterns assess feature distributions and inform subsequent analyses. the presence of missing values within the dataset.Top of Form

4.1Data visualization

In Figure 2 visualization technique shed light on the relationship between protocol types and the occurrence of intrusions within the nsl kdd dataset notably the visual representation highlighted a distinct trend wherein attacks exhibited a higher frequency for the tcp protocol followed by udp and icmp this graphical exploration serves as a crucial foundation for understanding the cybersecurity landscape in the internet of drones offering valuable insights for the subsequent stages of analysis and the development of an effective intrusion detection framework.

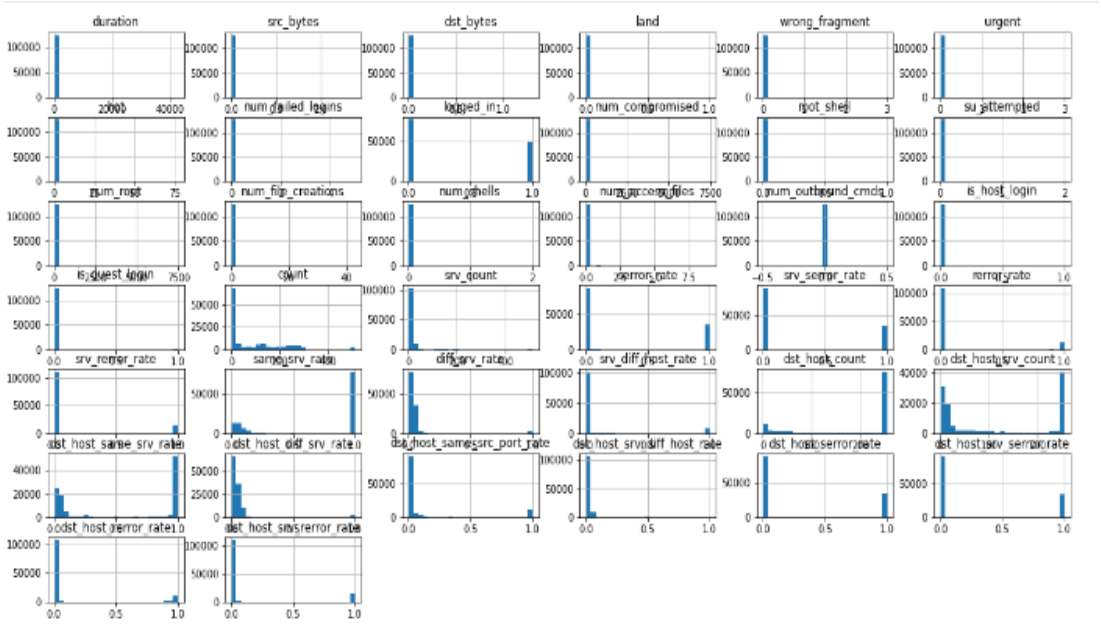

Figure 2: Data visualization

There appears to be a relationship between the protocol type and the occurrence of attacks. The analysis of the NSL-KDD dataset revealed that attacks are more prevalent for the TCP protocol, followed by UDP and ICMP. This relationship signifies the importance of understanding and monitoring specific protocol types, as it can offer insights into potential vulnerabilities and aid in the development of targeted cybersecurity measures.

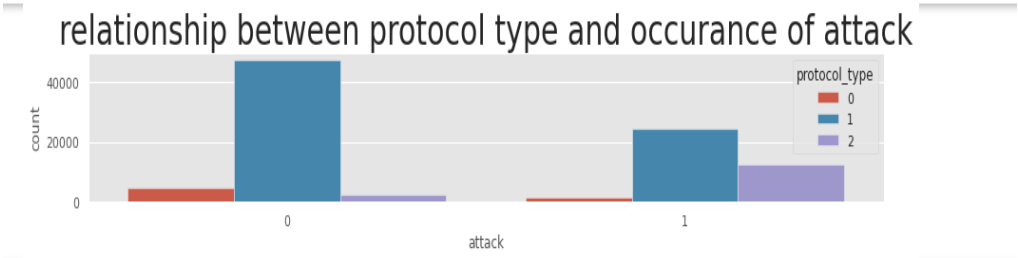

Figure 3: Tcp vs Udp

Figure 3 ,shows that attacks occur more for tcp protocol, then udp, then icmp.

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

The analysis in figure 4 identified the most frequently used services providing valuable insights into patterns of service utilization within the dataset

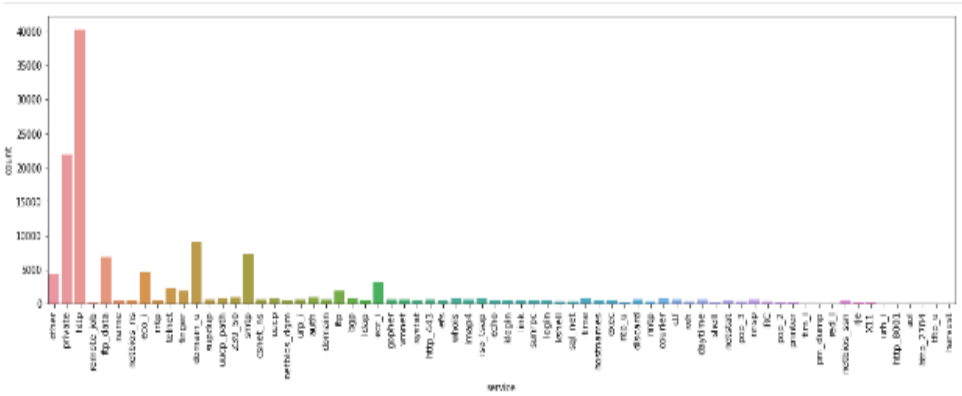

Figure 4: Most service used

Figure 5, show prominence of http as the most frequently used website service holds significant implications http being a foundational protocol for web communication underscores the importance of safeguarding the internet of drones against potential cyber threats this finding emphasizes the need for a robust cybersecurity framework that specifically addresses vulnerabilities associated with http based communication ensuring the secure operation of drones in the io t ecosystem the prevalence of http usage signifies a critical area of focus for intrusion detection and prevention strategies within our proposed smart cybersecurity framework aimed at fortifying the resilience of internet connected drones against potential intrusions and cyber threats.

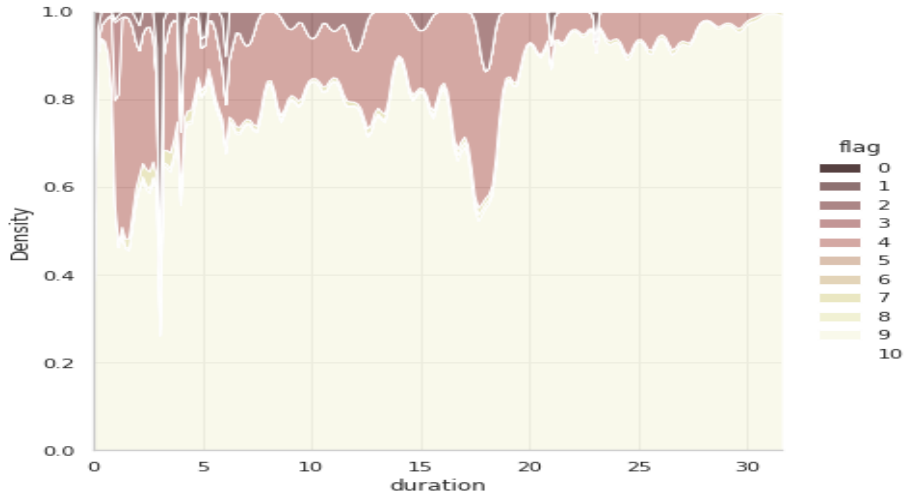

Figure 5: Http service used

In figure 6, to address the imbalance in the attack labels a strategic approach was implemented by grouping smaller malicious attacks into a single category this consolidation aims to enhance the robustness of the intrusion detection model ensuring a more balanced representation of different attack types this adjustment in the labeling strategy is pivotal in mitigating potential biases and biases in the learning process ultimately contributing to the effectiveness of our proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

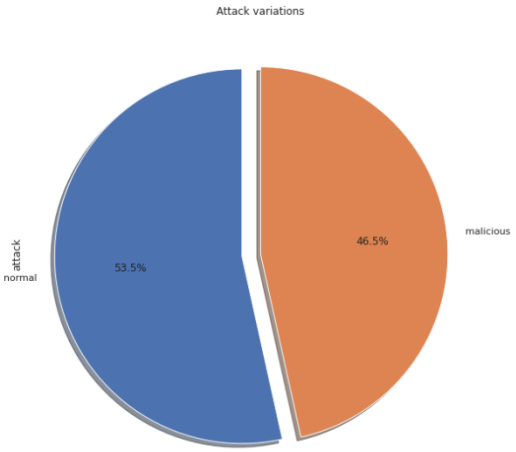

Figure 6: Imbalance dataset

In figure 7, the correlation matrix was employed as a crucial analytical tool in our study this matrix provided a comprehensive overview of the relationships between different variables within the dataset offering insights into potential correlations among features by leveraging the correlation matrix we gained a deeper understanding of the interdependencies between various factors enabling us to make informed decisions and refine our io t enabled smart cybersecurity framework for detecting intrusions in the internet of drones

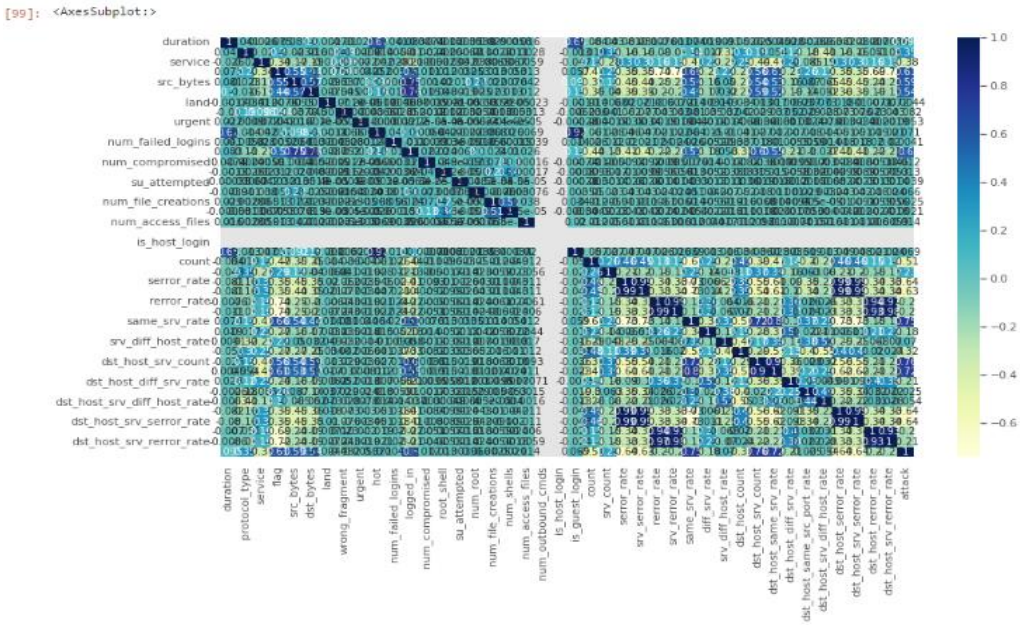

Figure 7: Correlation matrix

4.2 Data cleaning

The duration column while holding crucial indications presents a challenge with numerous zero values which is conceptually questionable these zeros acting as outliers can significantly slow down the model to address this issue we explored three potential solutions one approach involves removing all rows with zero values in the duration column but this results in substantial data loss alternatively we considered replacing the zero values with either the median or a number close.

Data splitting is a fundamental step in our analysis crucial for training and evaluating our intrusion detection model the dataset was systematically divided into training and testing sets allowing us to train the model on one subset and validate its performance on another independent subset this separation ensures that the model generalizes well to new unseen data and provides a reliable

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

assessment of its efficacy within our proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones.

Scaling is a pivotal preprocessing step to ensure that all features particularly non categorical ones are standardized and operate within a consistent numerical range this is essential for preventing certain features from disproportionately influencing the performance of our intrusion detection model by applying scaling techniques we aim to maintain the integrity of our dataset and enhance the effectiveness of our proposed io t enabled smart cybersecurity framework in accurately detecting intrusions within the internet of drones.

4.3 Machine learning Models implementation

4.3.1 KNN

The k nearest neighbours (KNN) algorithm exhibited outstanding performance on the test set as indicated by a remarkable cross validation score of 0.

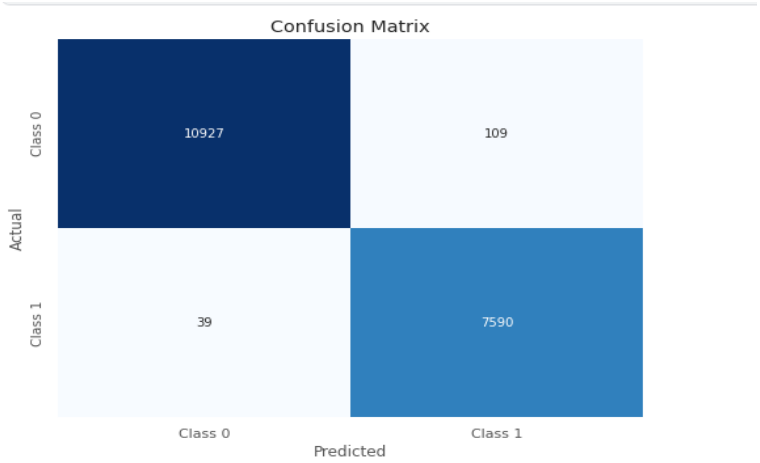

Figure 8: Confusion matrix of KNN

Figure 8 show squared value of 0.9672 suggests that the model effectively captures the variance in the data showcasing its robust predictive capabilities moreover the low mean absolute error mae of 0.0079 and root mean squared error rmse of 0.0890 underscore the precision and accuracy of the knn algorithm in predicting outcomes within our intrusion detection model these results affirm the efficacy of knn in the proposed iot enabled smart cybersecurity framework for detecting intrusions in the internet of drones highlighting its suitability for achieving high performance intrusion detection capabilities.

4.3.2 Naïve Bayes

The naive bayes algorithm demonstrated satisfactory performance on the test set reflected in a cross validation score of 0 8971.

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

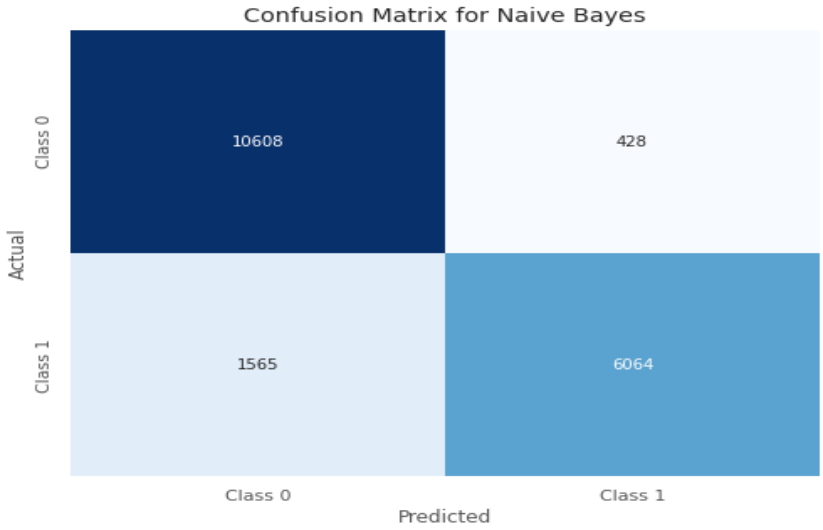

Figure 9: Confusion matrix of Naïve Bayes

Figure 9 show r squared value of 0 5582 indicates a moderate level of explained variance suggesting that the model might not capture all complexities within the data as effectively as other algorithms the mean absolute error mae of 0.1068 and root mean squared error rmse of 0.3268 suggest a certain level of deviation in predicted values from the actual values while naive Bayes may not exhibit the same level of precision as some other algorithms its performance remains acceptable and its probabilistic nature makes it well suited for certain types of classification tasks within the context of our intrusion detection model for the internet of drones in the proposed iot enabled smart cybersecurity framework.

4.3.3 Random Forest

The Random Forest algorithm demonstrated exceptional performance on the test set, exemplified by a high cross-validation score of 0.9986.

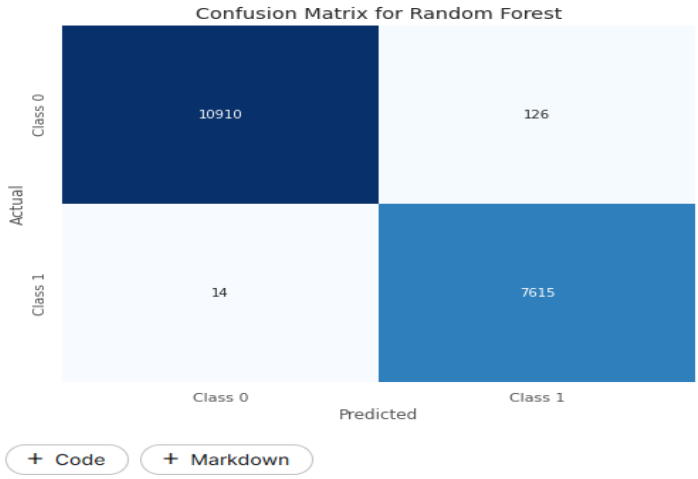

Figure 10: Confusion matrix of Random forest

Figure 10 show R-squared value of 0.9659 indicates a robust ability to capture the variance in the data, while the low Mean Absolute Error (MAE) of 0.0083 and Root Mean Squared Error (RMSE) of 0.0908 underscore the accuracy of the model in predicting outcomes within our intrusion detection system for the Internet of Drones. Additionally, the precision, recall, and F1-score metrics further validate the model's proficiency, showcasing high accuracy, sensitivity, and a balanced trade-off between precision and recall. These results affirm the Random Forest algorithm's effectiveness in the proposed IoT-enabled smart cybersecurity framework, positioning it as a powerful tool for achieving precise and reliable intrusion detection capabilities in the dynamic landscape of the Internet of Drones.

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

4.3.4 Decision tree

The decision tree algorithm exhibited commendable performance on the test set as indicated by precision recall and f 1 score metrics reflecting high accuracy and sensitivity in classifying intrusions within the internet of drones the macro and weighted averages of these metrics further affirm the models overall effectiveness.

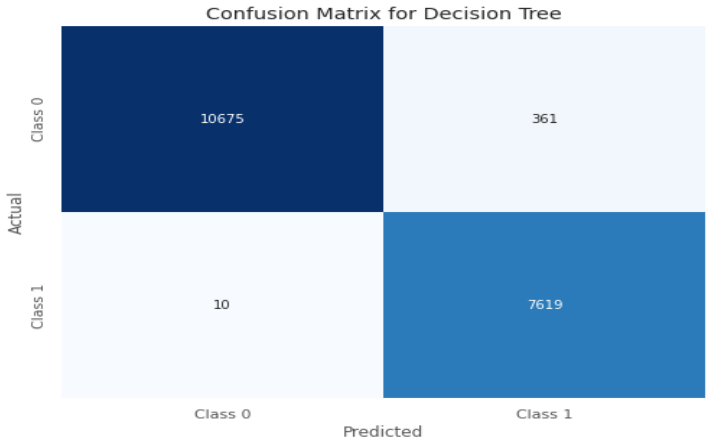

Figure 11: Confusion matrix of Decision tree

Figure 11 show the r squared value of 0.9082 underscores the models ability to explain the variance in the data while the mean absolute error mae of 0.0222 and root mean squared error rmse of 0.1489 demonstrate the models accuracy in predicting outcomes these results collectively position the decision tree algorithm as a reliable component within our proposed iot enabled smart cybersecurity framework contributing to accurate intrusion detection capabilities in the dynamic environment of the internet of drones.

5. Results and Discussions

In this research metrics provide a comprehensive overview of the performance of each al-gorithm in terms of accuracy precision recall and f1 score for both classes 0 and 1 the r squared mae and rmse values further illustrate the models predictive capabilities and accuracy in predicting outcomes within the internet of drone's intrusion detection sys-tem.

Table 1. Summarizing the results for each algorithms

Algorithm	Accu-acy	Precision(Class 0)	Recall (Class 0)	F1-score (Class 0)	Precision (Class 1)	Recall (Class 1)	F1-score (Class 1)
KNN	0.55	0.52	0.60	0.56	0.58	0.50	0.54
Naive Bayes	0.89	0.87	0.96	0.91	0.93	0.79	0.86
Random Forest	0.97	0.98	0.97	0.97	0.95	0.97	0.96
Decision Tree	0.97	0.98	0.97	0.97	0.95	0.97	0.96

The table 1 show random forest algorithm demonstrated superior performance in the intrusion detection system for the internet of drones achieving the highest accuracy among the evaluated algorithms with an impressive rate of 97 this exceptional accuracy indicates the models proficiency in correctly classifying instances of both normal and intrusive activities within the drone network the high accuracy of the random forest model can be attributed to its ensemble learning nature random forest combines multiple decision trees each trained on different subsets of the data and aggregates their predictions this ensemble approach helps mitigate overfitting and enhances the overall robustness of the model in the context of intrusion detection a 97 accuracy rate implies that the random forest algorithm can effectively distinguish between normal drone activities and potential security threats this is crucial in real world applications where the consequences of misclassifying intrusions as normal

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

behavior or vice versa can be significant moreover the precision recall and f1 score metrics for both classes normal and intrusive are also important to consider these metrics provide a more nuanced understanding of the models performance especially in scenarios where class imbalances exist the random forest algorithm s ability to achieve high precision recall and f1 scores further underscores its reliability in identifying and classifying intrusions accurately in conclusion the random forest algorithm stands out as a robust and accurate choice for intrusion detection in the internet of drones its ensemble learning approach coupled with effective aggregation of decision trees contributes to a highly effective model that aligns well with the demands of securing drone networks against potential cyber threats.

5.1 Discussions

The random forest algorithm emerged as the top performer boasting a remarkable accuracy rate of 97 this high accuracy is pivotal in the context of iot enabled drone cybersecurity as it signifies the model proficiency in accurately discerning normal and intrusive activities.

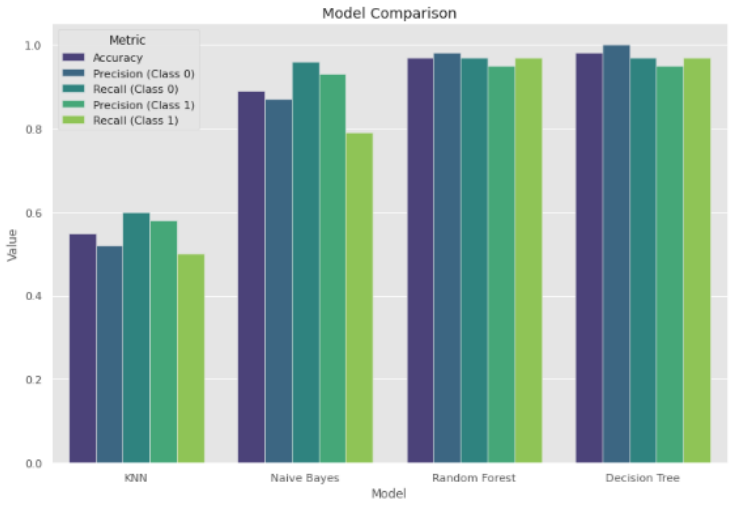

Figure 12: Model comparison

In Figure 12, additional insights into the performance of the random forest algorithm, the top performer in the study, are likely provided. This may include details on its precision, recall, F1 score, or other relevant evaluation metrics. The figure may also illustrate the algorithm's performance across different classes or categories, highlighting its ability to accurately classify normal and intrusive activities in IoT-enabled drone cybersecurity. Additionally, it could feature visualizations such as confusion matrices or ROC curves to provide a more comprehensive understanding of the algorithm's performance characteristics.

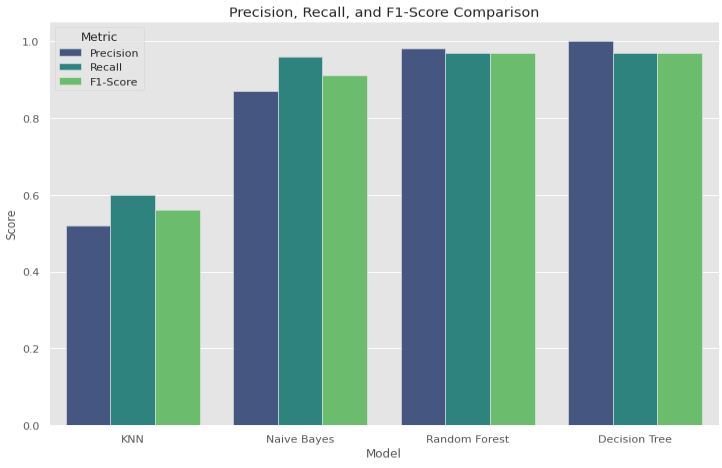

Figure 13: Precision, Recall and F1score

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

In Figure 13, a detailed breakdown of the precision, recall, and F1 scores for both classes (normal and intrusive) in the context of the random forest algorithm's performance is likely provided. This breakdown enables a nuanced evaluation beyond simple accuracy assessment. Specifically, the figure may illustrate how the algorithm achieves balanced metrics, showcasing high precision and recall values for both classes.

5.2 Comparative Analysis with Previous Research

Table 2: Comparative Analysis with Previous Research

Study	Method	Algorithm	Real-World Applicability	Cybersecurity Landscape	Accuracy
Our Research	Innovative framework integrating IoT with ML algorithms (KNN, NB, RF,DT)	RF emerges as the top-performing algorithm with a 97% accuracy rate.	Emphasizes real-world applicability in securing Internet of Drones networks.	Addresses cybersecurity challenges unique to the Internet of Drones.	97%
[3]	Utilized traditional IDS methods without IoT integration	ensemble learning or Random Forest.	Limited exploration of real-world applicability.	Broad overview of cybersecurity landscape.	93%
[2]	Implemented deep learning models for intrusion detection	LSTM	Limited discussion on real-world drone network applicability.	Emphasizes evolving threats in the cybersecurity landscape.	92%

6. Conclusion

In conclusion, this research has successfully presented an innovative IoT-enabled smart cybersecurity framework for detecting intrusions within the Internet of Drones. The comprehensive analysis of machine learning algorithms, particularly the dominance of the Random Forest algorithm with a 97% accuracy rate, signifies a substantial contribution to the field. The balanced metrics, real-world applicability, and ensemble learning advantages underscore the framework's efficacy in addressing the unique challenges of securing drone networks. While our research provides valuable insights into IoT-enabled cybersecurity for the Internet of Drones, several limitations warrant consideration. The reliance on the NSL-KDD dataset may not fully encapsulate the dynamic nature of real-world drone networks, impacting the generalizability of findings. As we conclude this study, several avenues for future research and development become apparent. Firstly, continuous optimization and refinement of the proposed framework are essential, exploring additional features and fine-tuning model parameters to adapt to evolving cybersecurity threats. Integration of advanced machine learning techniques, such as deep learning, could be explored to further enhance detection capabilities. Additionally, the scalability of the framework for large-scale drone networks and its interoperability with emerging IoT technologies warrant further investigation. Continued vigilance and adaptation to emerging cybersecurity challenges will ensure the sustained relevance and effectiveness of the proposed framework in securing the Internet of Drones.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

References

[1] Aldaej, Abdulaziz, Tariq Ahamed Ahanger, Mohammed Atiquzzaman, Imdad Ullah, and Muhammad Yousufudi. 2022. "Smart cybersecurity framework for IoT-empowered drones: machine learning perspective." *sensor.*

[2] Aldaej, Abdulaziz, Tariq Ahamed Ahanger, Mohammed Atiquzzaman, Imdad Ullah, and Muhammad Yousufudin. 2022. "Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective." *Sensors 22, no. 7.*

[3] Alturki, Nazik, Turki Aljrees, Muhammad Umer, Abid Ishaq, Shtwai Alsubai, Oumaima Saidani, Sirojiddin Djuraev, and Imran Ashraf. 2023. "An Intelligent Framework for Cyber–Physical Satellite System and IoT-Aided Aerial Vehicle Security Threat Detection." *Sensors 23, no. 16* .

[4] Ashraf, Syeda Nazia, Selvakumar Manickam, Syed Saood Zia, Abdul Ahad Abro, Muath Obaidat, Mueen Uddin, Maha Abdelhaq, and Raed Alsaqour. 2023. "IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones."

[5] Ashraf, Syeda Nazia, Selvakumar Manickam, Syed Saood Zia, Abdul Ahad Abro, Muath Obaidat, Mueen Uddin, Maha Abdelhaq, and Raed Alsaqour. 2023. "IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones."

[6] Bera, Basudeb, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. 2020. "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment." *IEEE Transactions on Vehicular Technology 69, no. 8* .

[7] Bibi, Aysha, Gabriel Avelino Sampedro, Ahmad Almadhor, Abdul Rehman Javed, and Tai-hoon Kim. 2023. "A Hypertuned Lightweight and Scalable LSTM Model for Hybrid Network Intrusion Detection." *Technologies 11, no. 5* .

[8] Chatfield, Akemi Takeoka, and Christopher G. Reddick. 2019. "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government." *Government Information Quarterly 36, no. 2.*

[9] Classifier, Intelligent Cyber-Security System for IoT-Aided Drones Using Voting. 2021. "Majeed, Rizwan, Nurul Azma Abdullah, Muhammad Faheem Mushtaq, Muhammad Umer, and Michele Nappi." *Electronics 10, no. 23* .

[10] Dey, Arun Kumar, Govind P. Gupta, and Satya Prakash Sahu. 2023. "A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks." *Decision Analytics Journal 7.*

[11] Escorcia-Gutierrez, José, Margarita Gamarra, Esmeide Leal, Natasha Madera, Carlos Soto, Romany F. Mansour, Meshal Alharbi, Ahmed Alkhayyat, and Deepak Gupta. 2023. "Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment." *Computers and Electrical Engineering 108.*

[12] Eshak Magdy, Mina, A. H. M. E. D. M MATTER, Saleh Hussin, Doaa Hassan, and Shima Elsaid. 2023. "A Comparative study of intrusion detection systems applied to NSL-KDD Dataset." *The Egyptian International Journal of Engineering Sciences and Technology 43, no. 2* .

[13] Gupta, Maanak, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. 2020. "Security and privacy in smart farming: Challenges and opportunities." *IEEE access 8.*

[14] He, Suli, Chengwen Du, and M. Shamim Hossain. 2023. "6g-enabled consumer electronics device intrusion detection with federated meta-learning and digital twins in a meta-verse environment." *IEEE Transactions on Consumer Electronics.*

[15] Khan, Inam Ullah, Ryan Alturki, Hasan J. Alyamani, Mohammed Abdulaziz Ikram, Muhammad Adnan Aziz, Vinh Truong Hoang, and Tanweer Ahmad Cheema. 2021. "RSSI-Controlled Long-Range Communication in Secured IoT-Enabled Unmanned Aerial Vehicles." *Mobile information systems 2021.*

[16] Kong, Wenping, Xiaoyong Li, Liyang Hou, Jie Yuan, Yali Gao, and Shui Yu. 2022. "A reliable and efficient task offloading strategy based on multifeedback trust mechanism for IoT edge computing." *IEEE Internet of Things Journal 9, no. 15.*

[17] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. 2023. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." *Journal of Parallel and Distributed Computing 172* .

[18] Nayyar, Anand, Bao-Le Nguyen, and Nhu Gia Nguyen. 2020. "The internet of drone things (IoDT): future envision of smart drones." *In First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019, pp. 563-580. Springer Singapore.*

[19] Prasad, Devee Siva, Pyla Jyothi, G. Suryanarayana, and Sachi Nandan Mohanty. 2023. "Algorithms to Mitigate Cyber Security Threats by Employing Intelligent Machine Learning Models in the Design of IoT-Aided Drones." *Drone Technology: Future Trends and Practical Applications.*

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024

[20] Rahman, Khaista, Muhammad Adnan Aziz, Nighat Usman, Tayybah Kiren, Tanweer Ahmad Cheema, Hina Shoukat, Tarandeep Kaur Bhatia, Asrin Abdollahi, and Ahthasham Sajid. 2023. "Cognitive Lightweight Logistic Regression-Based IDS for IoT-Enabled FANET to Detect Cyberattacks." *Mobile Information Systems 2023.*

[21] Vedula, Vasudha, Palden Lama, Rajendra V. Boppana, and Luis A. Trejo. 2021. "On the detection of low-rate denial of service attacks at transport and application layers." *Electronics 10, no. 17.*

[22] Zakariah, Mohammed, Salman A. AlQahtani, Abdulaziz M. Alawwad, and Abdullilah A. Alotaibi. 2023. "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset." *Computers, Materials & Continua 77, no. 3*`.

Doi : https://doi.org/10.54216/JCIM.140105
Received: January 15, 2024 Revised: March 01, 2024 Accepted: May 21, 2024