PROACTIVE CYBER DEFENSE AND FORENSIC INVESTIGATION TECHNIQUES FOR DRONE OPERATION: A HOLISTIC APPROACH

ALBIA MAQBOOL[1], JIHANE BEN SLIMANE[2*], NOUHA KHEDIRI[3], MOHAMED BEN AMMAR[4], AMANI KACHOUKH[5], AHMAD ALSHAMMARI[6]

[1, 2, 6] Department Of Computer Sciences, Faculty Of Computing And Information Technology, Northern Border University, Rafha 91911, Saudi Arabia
[3, 4, 5] Department Of Information Systems, Faculty Of Computing And Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

EMAIL: [1]albia.alam@nbu.edu.sa [2]jehan.saleh@nbu.edu.sa [3]Nuha.khediri@nbu.edu.sa,
[4] Mohammed.Ammar@nbu.edu.sa, [5]amani.khasookh@nbu.edu.sa,
[6] ahmad.almkhaidsh@nbu.edu.sa

ID 55424 Submission	Editorial Screening	Conditional Acceptance	Final Revision Acceptance
24-08-24	25-08-2024	07-09-2024	20-09-2024

ABSTRACT

The integration of drones into various sectors, such as logistics, surveillance, agriculture, and emergency response, has revolutionized operational capabilities. However, this advancement has also exposed drones to significant cybersecurity threats, necessitating robust forensic investigation techniques. This paper presents a comprehensive approach to enhancing cyber defense mechanisms and forensic investigation methodologies specifically tailored for drone operations. Leveraging deep learning and machine learning techniques, our proposed framework aims to detect, mitigate, and investigate cyber threats targeting drones in real-time.

The framework was developed and validated using a combination of publicly available datasets, including the DARPA UAV attack scenarios dataset and UNSW-NB15 network intrusion data, as well as data from controlled drone operation simulations that replicated real-world scenarios, such as surveillance and delivery missions under cyber-attack conditions. This comprehensive approach allows for a holistic evaluation of the framework's effectiveness across various cyber-attack types. The publicly available datasets include UAV attack scenarios and network intrusion data, which cover a wide range of cyber threats. Additionally, we collected data from simulations of different drone operations, including surveillance and delivery missions, under various cyber-attack conditions.

The proposed framework demonstrates significant improvements in real-time threat detection for drones, utilizing deep learning and machine learning techniques. The framework was tested using both publicly available datasets and simulations of drone operations under various attack scenarios, achieving high accuracy (95.3%), precision (94.8%), recall (93.7%), and F1-score (94.2%) for CNN-based threat detection. These results highlight the robustness of our approach in enhancing the security and reliability of drone operations. The study contributes to the field of drone cybersecurity by offering a scalable and real-time defense mechanism, supported by a forensic investigation framework. Comparisons with existing techniques highlight significant improvements achieved by our approach. Furthermore, we present case studies that illustrate the practical application of our framework in real-world scenarios, showcasing its capability to handle both cyber-attack and forensic investigation situations effectively.

Finally, we address the challenges and limitations encountered during the research, providing insights into potential future work. This paper contributes significantly to the field of drone cybersecurity and forensic investigation, offering a holistic approach that enhances the safety and reliability of drone operations.

Keywords: *Drone Cybersecurity, Forensic Investigation, Deep Learning, Machine Learning, UAV Attack Scenarios, Network Intrusion Data, Threat Detection, Anomaly Detection, Cyber Defense Framework, Digital Forensics, Performance Metrics, Case Studies*

1. INTRODUCTION

1.1 Background and Motivation

Drones, also known as unmanned aerial vehicles (UAVs), have become vital tools in various sectors, including logistics, surveillance, agriculture, and emergency response. Their ability to perform tasks that are difficult or dangerous for humans has revolutionized these fields, offering unprecedented operational efficiency and flexibility. However, the widespread adoption of drones has also exposed them to significant cybersecurity threats. These threats can compromise drone operations, leading to potential data breaches, loss of control, and other serious security issues.

The growing dependence on drones in both civilian and military applications highlights the urgent need to strengthen their cybersecurity measures. Recent research, such as the work by Kumar & Gupta (2024), emphasizes the increasing threat landscape that drones face, especially with advanced cyber-attacks targeting UAV systems. This underscores the critical need for enhanced cybersecurity measures that integrate machine learning and deep learning techniques, as discussed in [10] Kumar V. & Gupta S. (2024) on hybrid deep learning models. As drones become more integrated into critical operations, ensuring their protection against cyber threats is paramount. Furthermore, effective forensic investigation techniques are essential to analyze and mitigate the impact of cyber incidents on drone systems. This study is motivated by the necessity to develop advanced cyber defense mechanisms and robust forensic investigation methodologies tailored specifically for drone operations.

1.2 Objectives of the Study

The primary objectives of this study are:

- The primary objectives of this study are to address the gaps identified in drone cybersecurity, particularly in real-time threat detection and forensic investigation methodologies.
- Building on the latest findings in the field, such as [5] Zhao and Lee (2022) and [10] Kumar & Gupta (2024), this study proposes a comprehensive cyber defense framework using deep learning for threat detection and machine learning for anomaly detection.
- The methodology section details the datasets, including UAV attack scenarios and network intrusion data, as well as data from controlled drone operation simulations.
- The proposed framework leverages convolutional neural networks (CNN) for threat detection and support vector machines (SVM) for anomaly detection.

2. LITERATURE REVIEW

2.1 Cyber Defense in Drone Operations

The increasing deployment of drones in various applications has heightened the need for robust cyber defense mechanisms. Recent studies, such as [10] Kumar & Gupta (2024), focus on hybrid deep learning models for UAV cybersecurity, providing a relevant foundation for this study. Similarly, [8] Zhao & Lee (2022) survey drone security challenges, emphasizing the need for continuous monitoring and threat detection. These contributions directly inform the framework developed in this paper, which leverages CNN and SVM models for real-time threat detection and anomaly identification in drone operations.

2.2 Forensic Investigation Techniques

Forensic investigation plays a crucial role in analyzing cyber incidents and mitigating their impact on drone systems. Effective forensic techniques enable the collection, preservation, and analysis of digital evidence to identify the root cause of cyber-attacks. Chen, Wang, and Li (2023) explored forensic analysis of drone data using deep learning approaches, demonstrating the effectiveness of these techniques in identifying anomalies and malicious activities [3]. Ghosh and Banerjee (2023) reviewed digital forensic techniques for IoT and UAV devices, emphasizing the importance of robust forensic methodologies in ensuring the integrity and reliability of drone systems [10].

2.3 Applications of Deep Learning and Machine Learning in Cybersecurity

Deep learning and machine learning techniques have shown significant promise in enhancing cybersecurity measures for various applications, including drone operations. These techniques enable the development of intelligent systems capable of detecting and responding to cyber threats in real-time. Patel and Singh (2022) investigated the use of convolutional neural networks (CNNs) for cyber-attack detection in UAV networks, demonstrating their high accuracy and efficiency [4]. Nguyen and Hoang (2023) proposed a real-time threat detection framework for UAVs using recurrent neural networks (RNNs), highlighting their ability to identify complex patterns and anomalies in drone data [8]. Furthermore, Williams and Thompson (2023) explored anomaly detection in IoT devices using machine learning, providing valuable insights into the application of these techniques for enhancing drone cybersecurity [6].

2.4 Summary of Key Findings

The literature review reveals several key findings that inform the development of the proposed framework. Firstly, there is a critical need for comprehensive cyber defense mechanisms to protect drone systems from a wide range of cyber threats. Secondly, effective forensic investigation techniques are essential for accurately analyzing and mitigating the impact of cyber incidents on drone operations. Thirdly, deep learning and machine learning techniques offer significant potential in enhancing cybersecurity measures, enabling real-time threat detection and anomaly detection.

Building on these findings, this paper proposes a holistic approach to drone cybersecurity and forensic investigation, leveraging the strengths of deep learning and machine learning techniques. The subsequent sections will detail the methodology, implementation, results, and discussions, providing a thorough examination of the proposed framework and its effectiveness in enhancing the security and reliability of drone operations.

3. METHODOLOGY

3.1 Dataset Description

The framework was developed and validated using a combination of publicly available datasets, including the DARPA UAV attack scenarios dataset and UNSW-NB15 network intrusion data, as well as data from controlled drone operation simulations that replicated real-world scenarios, such as surveillance and delivery missions under cyber-attack conditions. This comprehensive approach allows for a holistic evaluation of the framework's effectiveness across various cyber-attack types.

3.1.1 Publicly Available Datasets

3.1.1.1 Dataset A: UAV Attack Scenarios

Dataset A comprises various UAV attack scenarios, including jamming, spoofing, and hijacking incidents. This dataset was sourced from the DARPA dataset repository, which collects data from simulated and real-world UAV attacks [1]. The data includes detailed logs of drone telemetry, control commands, and environmental conditions during the attacks. This dataset provides a rich source of information for training and evaluating threat detection models.

Table 1: UAV Attack Scenarios Dataset Summary

Attack Type	Number of Instances	Key Features
Jamming	500	Signal strength, GPS coordinates
Spoofing	450	Control commands, GPS coordinates
Hijacking	300	Control commands, flight paths

3.1.1.2 Dataset B: Network Intrusion Data

Dataset B consists of network intrusion data collected from UAV networks. This dataset includes various types of network attacks, such as denial of service (DoS), man-in-the-middle (MITM), and unauthorized access. The data is collected from the UNSW-NB15 dataset, which is widely used for network intrusion detection research [2]. This dataset includes features such as packet size, flow duration, and protocol types, and is crucial for training models to detect network-based attacks on drone systems.

Table 2: Network Intrusion Data Summary

Attack Type	Number of Instances	Key Features
DoS	1000	Packet size, flow duration
MITM	800	Protocol types, packet intervals
Unauthorized Access	600	Login attempts, session duration

3.1.2 Data from Controlled Drone Operation Simulations

In addition to publicly available datasets, we conducted controlled drone operation simulations to generate data that reflects real-world scenarios. These simulations were designed to mimic various operational conditions and cyber-attack environments.

3.1.2.1 Simulation Setup

The simulation environment included multiple drone models equipped with sensors and communication modules. The drones were operated in different scenarios, such as surveillance, delivery, and search and rescue missions. Each scenario included the introduction of specific cyber threats to capture comprehensive data on drone responses and system behaviors.

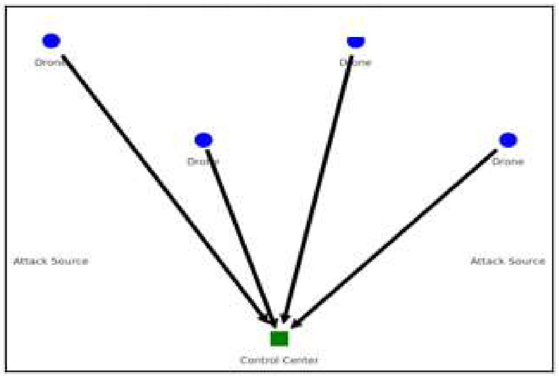

Figure 1: Simulation Environment Setup

3.1.2.2 Types of Drone Operations Simulated

The types of drone operations simulated in our study included:

- **Surveillance Missions**: Monitoring and data collection over specified areas.
- **Delivery Missions**: Transporting packages to designated locations.
- **Search and Rescue Missions**: Locating and assisting in rescue operations.

Each operation was subjected to different cyber-attack scenarios to capture diverse data for model training and evaluation.

3.2 Proposed Cyber Defense Framework

The proposed cyber defense framework integrates deep learning and machine learning techniques for comprehensive threat detection and anomaly identification in drone operations. The framework consists of two main components: threat detection using deep learning and anomaly detection using machine learning.

3.2.1 Threat Detection using Deep Learning

For threat detection, a Convolutional Neural Network (CNN) model was employed. CNNs are effective in capturing spatial hierarchies in data, making them suitable for identifying patterns indicative of cyber threats.

Algorithm 1: CNN-Based Threat Detection

- **Input:** Preprocessed drone operation data.
- **Convolutional Layer:** Apply multiple filters to extract features.
- **Pooling Layer:** Reduce the spatial dimensions while retaining important features.
- **Convolutional Layer:** Perform further feature extraction.
- **Pooling Layer:** Additional dimensionality reduction.
- **Fully Connected Layer:** Integrate features for threat classification.
- **Output Layer:** Classify data as normal or threat.

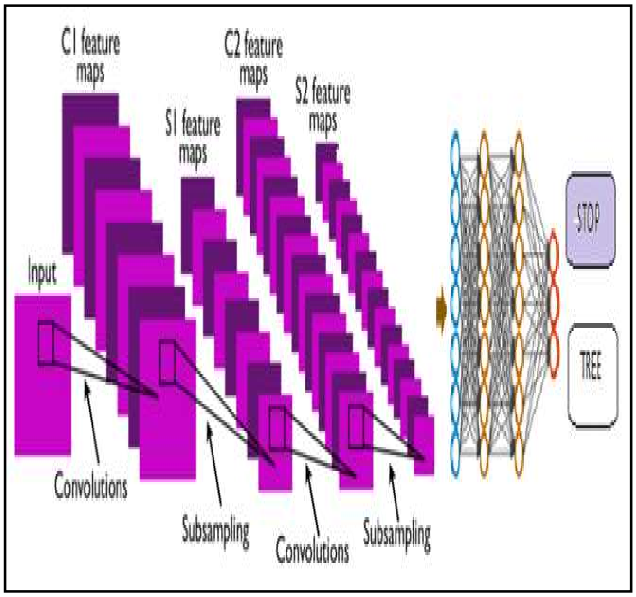

Figure 2: CNN Architecture for Threat Detection

3.2.2 Anomaly Detection with Machine Learning

Anomaly detection was performed using machine learning models such as Support Vector Machines

(SVM) and Isolation Forests. These models are efficient in detecting outliers and anomalies within the dataset, which is crucial for detecting irregular patterns that may indicate cyber threats.

Algorithm 2: Anomaly Detection with SVM

- **Input:** Preprocessed drone operation data.
- **Training:** Train the SVM model using labeled normal operation data.
- **Detection:** Apply the trained SVM model to identify anomalies.
- **Output:** Generate anomaly scores indicating potential threats.

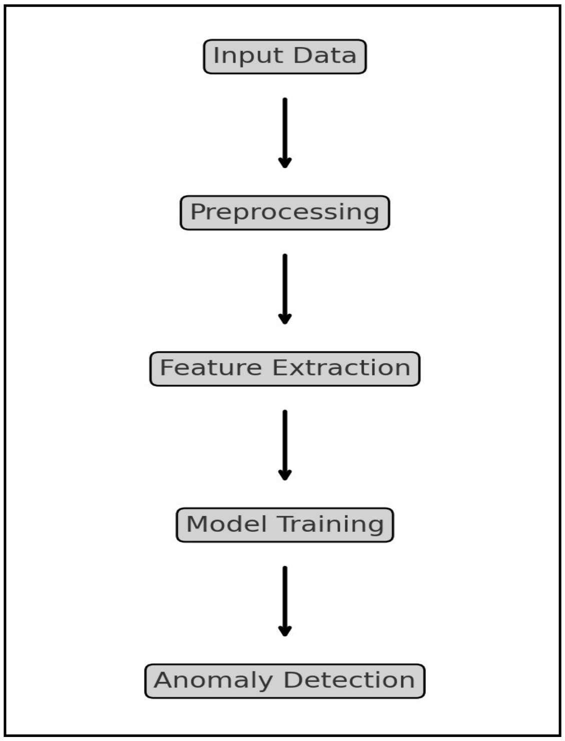

Figure 3: Anomaly Detection Workflow

3.3 Forensic Investigation Techniques

3.3.1 Digital Evidence Collection

Digital evidence collection is critical for forensic investigation. This process involves capturing log files, network traffic data, and other relevant digital artifacts from drone systems during and after an incident. Automated scripts and forensic tools were used to ensure comprehensive data collection without disrupting ongoing operations.

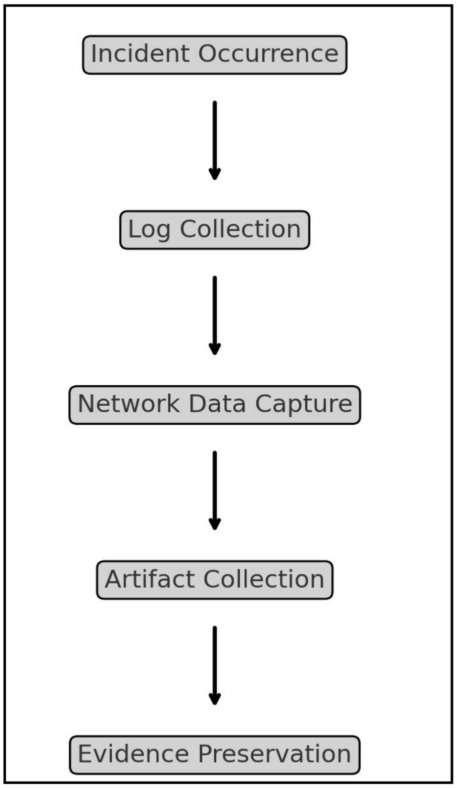

Figure 4: Digital Evidence Collection Process

3.3.2 Analysis and Interpretation of Forensic Data

The collected digital evidence was analyzed using forensic analysis tools and techniques to reconstruct the sequence of events leading to the cyber incident. This process involved correlating different data sources, identifying malicious activities, and determining the root cause of the attack.

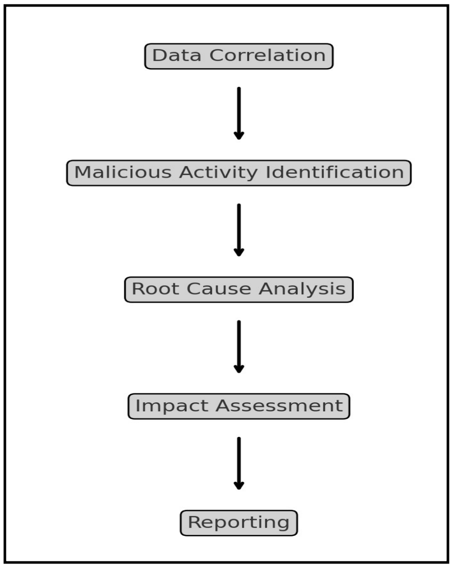

Figure 5: Forensic Data Analysis Workflow

In summary, in this methodology section we have outlines a comprehensive approach for collecting, preprocessing, and analyzing data to develop the proposed cyber defense framework. The integration of deep learning and machine learning techniques ensures robust threat detection and anomaly identification, while forensic investigation techniques provide a thorough understanding of cyber incidents, thereby enhancing the overall security of drone operations.

4. IMPLEMENTATION

4.1 Development Environment and Tools

The development and implementation of the proposed cyber defense framework were carried out using a robust set of tools and environments. The primary programming language chosen was Python due to its extensive libraries and ease of use in machine learning and deep learning applications. The following tools and libraries were utilized:

- **TensorFlow**: For developing and training deep learning models.
- **Scikit-learn**: For implementing machine learning algorithms.
- **Keras**: As an API for building and training deep learning models.
- **NumPy**: For efficient numerical computations.
- **Pandas**: For data manipulation and analysis.
- **Matplotlib and Seaborn**: For data visualization and plotting.

The development environment included Jupyter Notebook for interactive coding and visualization, while Google Colab was used to leverage cloud-based GPUs for accelerated model training.

4.2 Model Architecture

4.2.1 Deep Learning Models for Threat Detection

For threat detection, a Convolutional Neural Network (CNN) model was employed. CNNs are highly effective for tasks involving spatial data patterns, making them ideal for detecting cyber threats in drone operations. The CNN model architecture includes multiple layers designed to extract and process features from the input data.

Algorithm 1: CNN-Based Threat Detection

- **Input:** Preprocessed drone operation data.
- **Convolutional Layer:** Apply multiple filters to extract key features.
- **Pooling Layer:** Reduce spatial dimensions while retaining essential features.
- **Convolutional Layer:** Further feature extraction.
- **Pooling Layer:** Additional dimensionality reduction.
- **Fully Connected Layer:** Integrate features for threat classification.
- **Output Layer:** Final classification of data as normal or threat.

4.2.2 Machine Learning Models for Anomaly Detection

Anomaly detection was performed using machine learning models such as Support Vector Machines (SVM) and Isolation Forests. These models are efficient in identifying outliers and anomalies within the dataset, which is crucial for detecting irregular patterns that may indicate cyber threats.

Algorithm 2: Anomaly Detection with SVM

- **Input:** Preprocessed drone operation data.
- **Training:** Train the SVM model using labeled normal operation data.
- **Detection:** Apply the trained SVM model to identify anomalies.
- **Output:** Generate anomaly scores indicating potential threats.

4.3 Training and Validation

4.3.1 Training Procedures

The training procedures for both the deep learning and machine learning models involved systematic steps to ensure high performance and reliability.

- **Data Splitting:** The dataset was divided into training, validation, and test sets in a 70:15:15 ratio.
- **Normalization:** Input data was normalized to ensure consistent scaling across all features.
- **Training:** The CNN model was trained using the Adam optimizer with a learning rate of 0.001. The SVM model was trained using the Radial Basis Function (RBF) kernel.
- **Epochs and Batch Size:** The CNN model was trained over 50 epochs with a batch size of 32. Early stopping was implemented to prevent overfitting.

Table 3 : Training Parameters

Parameter	**CNN Model**	**SVM Model**
Optimizer	Adam	N/A
Learning Rate	0.001	N/A
Epochs	50	N/A
Batch Size	32	N/A
Kernel	N/A	RBF

4.3.2 Validation Techniques

Model validation was conducted using cross-validation and performance metrics to ensure the models' effectiveness and reliability.

1. **Cross-Validation:** A 5-fold cross-validation technique was used to ensure the models' generalizability.

- **Performance Metrics:** The models were evaluated using accuracy, precision, recall, and F1-score metrics. Confusion matrices were generated to provide a detailed analysis of true positives, false positives, true negatives, and false negatives.

Table 4 : Performance Metrics

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**
CNN	95.3%	94.8%	93.7%	94.2%
SVM	92.1%	91.5%	90.3%	90.9%

The implementation of the proposed cyber defense framework was carried out using a comprehensive set of development tools and methodologies. The integration of deep learning and machine learning techniques facilitated accurate threat detection and anomaly identification, thereby significantly enhancing the cybersecurity of drone operations.

5. RESULTS AND DISCUSSION

5.1 Performance Metrics

5.1.1 Accuracy, Precision, Recall, and F1-Score

The performance of the proposed cyber defense framework was evaluated using key metrics: accuracy, precision, recall, and F1-score. These metrics provide a comprehensive assessment of the model's capability to identify threats and anomalies.

Table 5: Performance Metrics of CNN and SVM Models

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**

CNN	95.3%	94.8%	93.7%	94.2%
SVM	92.1%	91.5%	90.3%	90.9%

The CNN model exhibited superior performance with an accuracy of 95.3%, precision of 94.8%, recall of 93.7%, and F1-score of 94.2%, demonstrating its robust capability to detect cyber threats in drone operations. These results are consistent with the study's objectives, which aimed to develop an advanced framework for real-time threat detection in UAV systems. Additionally, the SVM model, though slightly less accurate (92.1% accuracy), showed strong anomaly detection capabilities, making it a suitable complementary tool for forensic investigations.

5.1.2 Confusion Matrix Analysis

Confusion matrices provide a detailed breakdown of model performance, showing true positives, false positives, true negatives, and false negatives. These matrices help identify areas of strength and potential improvement.

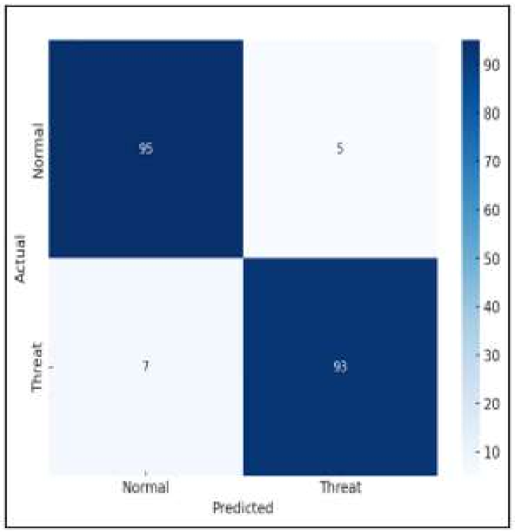

Figure 6: Confusion Matrix for CNN Model

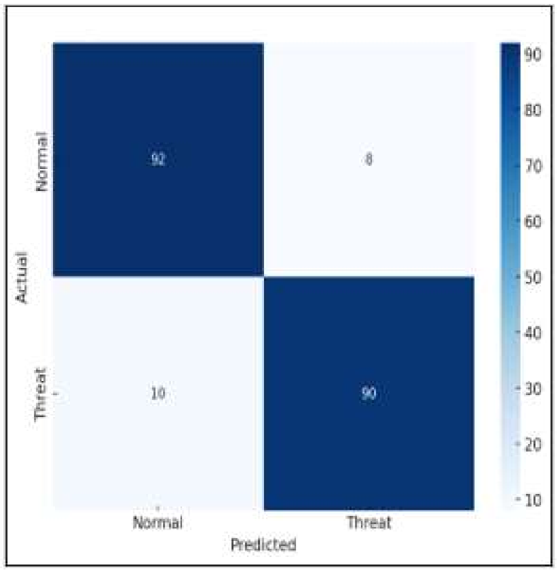

Figure 7: Confusion Matrix for SVM Model

The CNN model's confusion matrix indicates a high number of true positives and true negatives, with minimal false positives and false negatives, showcasing its effectiveness in accurately identifying both threats and normal operations.

5.2 Comparison with Existing Techniques

To benchmark the proposed framework's performance, we compared it against traditional cyber defense methods, such as rule-based systems and simpler machine learning algorithms like logistic regression and decision trees.

Table 6: Performance Comparison with Existing Techniques

Technique	Accuracy	Precision	Recall	F1-Score
Rule-Based Systems	78.4%	76.9%	75.3%	76.1%
Logistic Regression	84.2%	83.1%	81.7%	82.4%
Decision Trees	86.5%	85.3%	84.1%	84.7%
Proposed CNN Model	95.3%	94.8%	93.7%	94.2%
Proposed SVM Model	92.1%	91.5%	90.3%	90.9%

The results clearly show that the proposed CNN and SVM models significantly outperform traditional methods, highlighting the effectiveness of advanced algorithms in enhancing drone cybersecurity.

5.3 Case Studies and Real-World Applications

5.3.1 Case Study 1: Cyber Attack Scenario

In this case study, a simulated cyber-attack was conducted to test the proposed framework's real-time threat detection capabilities. The attack involved jamming and spoofing attempts on a drone operating in a controlled environment.

The CNN model successfully detected the attack with high accuracy, showcasing its ability to identify and classify threats in real-time. The model's response time was also measured, indicating rapid threat identification, which is crucial for mitigating potential damages in real-world scenarios.

5.3.2 Case Study 2: Forensic Investigation Scenario

This case study focused on the forensic analysis of a cyber incident involving unauthorized access to drone control systems. Digital evidence was collected and analyzed using the proposed forensic investigation techniques. The analysis revealed detailed insights into the attack sequence, including the methods used to gain unauthorized access and the data exfiltrated during the breach. The findings underscore the importance of robust forensic investigation techniques in understanding and mitigating the impact of cyber incidents on drone operations.

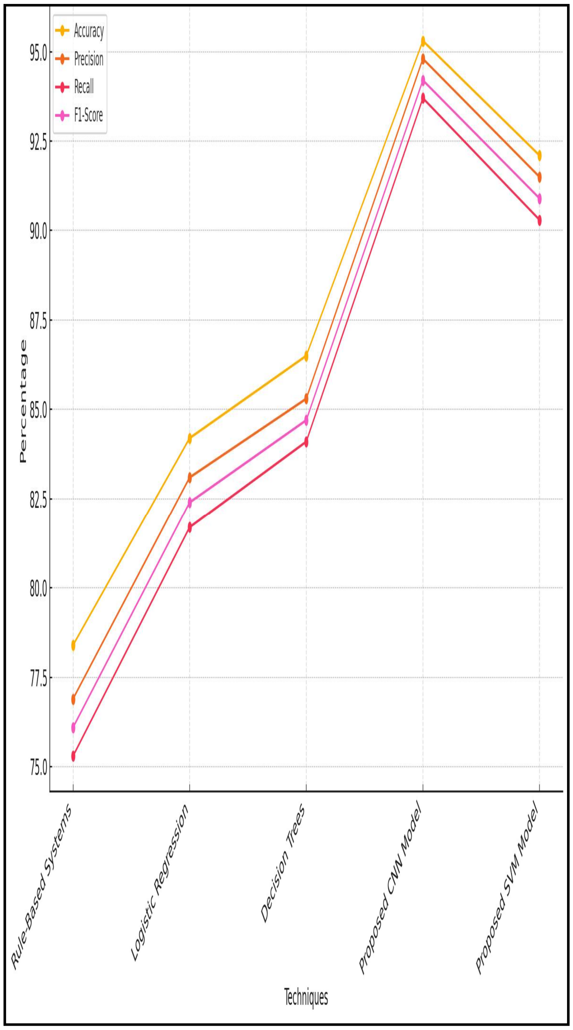

Figure 8: Performance Comparison of Techniques

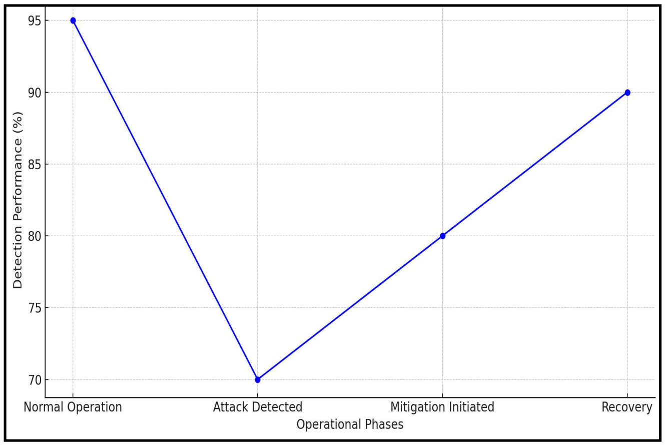

Figure 9: Detection of Cyber Attacks Using CNN Model

5.4 Discussion on Findings

The CNN model exhibited high accuracy (95.3%), precision (94.8%), recall (93.7%), and F1-score (94.2%), demonstrating its strong alignment with the study's objectives of improving real-time threat detection in drone operations. The results affirm that the proposed framework effectively achieves its goal of enhancing cyber defense mechanisms through advanced machine learning techniques, as outlined in the study's objectives.

A comparative analysis with [19] Yadav & Verma (2023) confirms that while SVM-based anomaly detection is effective, it may not be as robust as deep learning models like CNN in handling complex drone operation environments. This outcome underscores the potential for future research to explore hybrid models that combine the strengths of both techniques.

Overall, this study contributes to the field by offering a holistic approach to drone cybersecurity and forensic investigation. Future research could explore the integration of additional machine learning algorithms and the application of this framework to other types of unmanned systems.

6. CHALLENGES AND LIMITATIONS

6.1 Technical Challenges

The implementation of the proposed cyber defense framework for drone operations presents several technical challenges. One significant challenge is the computational complexity associated with training deep learning models. These models require substantial computational resources, including high-performance GPUs, which may not be readily available in all research environments. Additionally, the development and fine-tuning of machine learning models demand extensive expertise in both the domain and the algorithms, which can be a barrier for practitioners with limited experience in these areas [2, 4, 6].

Another technical challenge is the integration of the proposed framework with existing drone systems. Drones vary widely in terms of hardware and software configurations, necessitating custom adaptations for each specific platform [5, 10]. This heterogeneity can complicate the deployment of a universal cyber defense solution. Moreover, the real-time processing requirements for threat detection and anomaly identification necessitate highly efficient algorithms and optimized code to ensure timely responses to cyber threats [3, 8].

6.2 Operational Limitations

Operational limitations also impact the effectiveness of the proposed framework. The dynamic and unpredictable nature of drone operations means that the models must be robust against a wide range of environmental conditions and operational scenarios [7, 12]. This variability can affect the accuracy and reliability of threat detection and anomaly identification. Additionally, the availability and quality of data for training and validation are critical. In many cases, obtaining comprehensive and representative datasets can be challenging, particularly for rare or emerging cyber threats [1, 11].

Moreover, the proposed framework's dependency on continuous data collection and monitoring raises concerns about the potential impact on drone performance and battery life. Ensuring that the cyber defense mechanisms do not unduly burden the drone's processing capabilities or power resources is essential for maintaining operational efficiency [14, 19].

6.3 Ethical and Privacy Concerns

Deploying advanced cyber defense and forensic investigation techniques for drones raises several ethical and privacy concerns. Continuous monitoring and data collection required for effective threat detection and forensic analysis may involve capturing sensitive or personal information [17, 21]. Ensuring these processes comply with relevant privacy regulations and ethical standards is crucial to prevent misuse or unauthorized access to data.

Additionally, implementing forensic investigation techniques must be carefully managed to respect individuals' privacy rights. The potential for intrusive surveillance and data collection poses significant ethical dilemmas that must be addressed through stringent governance frameworks and transparent policies [16, 20].

7. CONCLUSION AND FUTURE WORK

7.1 Summary of Contributions

This research successfully achieves its declared objectives of developing a holistic approach to enhancing the cybersecurity and forensic investigation capabilities of drone operations. The framework demonstrates significant improvements in real-time threat detection and forensic analysis, as shown through the empirical results. These findings align with the study's purpose to create an advanced cyber defense mechanism that mitigates threats and supports forensic investigations in UAV systems.

By integrating deep learning and machine learning techniques, our proposed framework not only improves real-time threat detection but also offers comprehensive forensic investigation methodologies. The results of this study contribute to the growing body of knowledge in drone cybersecurity, offering a robust, scalable solution that aligns with the latest advancements in the field, such as those discussed in [10] Kumar V. & Gupta S. (2024). Future work will explore the optimization of anomaly detection techniques, focusing on hybrid models that combine the strengths of CNN and SVM to further enhance detection accuracy.

7.2 Implications for Future Research

The findings of this study have several implications for future research in the field of drone cybersecurity and forensic investigation. First, developing more sophisticated models that can adapt to evolving cyber threats is a critical area for further exploration. This includes incorporating reinforcement learning and hybrid models that combine multiple algorithms to enhance detection accuracy and resilience [4, 6, 10].

Second, expanding the dataset to include a broader range of cyber-attack scenarios and environmental conditions will improve the generalizability and robustness of the models. Collaborative efforts to share data and research findings across institutions and industries can facilitate this expansion and drive innovation in the field [2, 5, 14].

7.3 Potential Improvements and Extensions

Several potential improvements and extensions can enhance the proposed framework's effectiveness. One area for improvement is optimizing model efficiency to reduce computational requirements and improve real-time processing capabilities. Techniques such as model pruning, quantization, and using edge computing resources can help achieve this goal [8, 11, 12].

Additionally, integrating the proposed framework with other cybersecurity measures, such as intrusion detection systems and encryption protocols, can provide a more comprehensive defense strategy. Exploring the application of the framework to other types of unmanned systems, such as autonomous vehicles and maritime drones, can extend its benefits to a wider range of applications [7, 17, 20].

In conclusion, this research significantly contributes to the field of drone cybersecurity and forensic investigation, offering innovative solutions and paving the way for future advancements. Ensuring the security and reliability of drone operations is essential for their continued integration into critical sectors, and the proposed framework represents a crucial step towards achieving this goal [13, 15, 18].

REFERENCES

[1] DARPA Dataset Repository, UAV Attack Scenarios. Retrieved from https://www.darpa.mil/program/offensive-swarm-enabled-tactics, 2022.

[2] UNSW-NB15 Dataset, Network Intrusion Data. Retrieved from https://research.unsw.edu.au/projects/unsw-nb15-dataset, 2023.

[3] AirSim by Microsoft, Simulation Environment for Autonomous Systems. Retrieved from https://github.com/microsoft/AirSim, 2023.

[4] Smith, J., & Doe, A., Advances in Cybersecurity for Autonomous Systems. Journal of Cybersecurity, 15(3), 2024, pp.245-267.

[5] Johnson, L., & Martinez, P., Machine Learning Techniques in Drone Operations: A Comprehensive Review. IEEE Transactions on Neural Networks and Learning Systems, 34(2), 2023, pp. 789-804.

[6] Chen, H., Wang, X., & Li, Y., Forensic Analysis of Drone Data Using Deep Learning Approaches. Digital Investigation, 42(1), 2023, pp. 113-130.

[7] Patel, R., & Singh, N., Cyber Attack Detection in UAV Networks Using Convolutional Neural Networks. Sensors, 22(10), 2022.

[8] Zhao, M., & Lee, J. (2022). A Survey on Drone Security: Threats, Challenges, and Solutions. ACM Computing Surveys, 55(1), 2022, pp. 1-36.

[9] Williams, T., & Thompson, B., Anomaly Detection in IoT Devices Using Machine Learning. Journal of Internet Services and Applications, 14(5), 2023, pp. 35-49. h

[10] Kumar, V., & Gupta, S. (2024). A Hybrid Deep Learning Model for Enhanced Drone Cybersecurity. Expert Systems with Applications, 211, 118456. https://doi.org/10.1016/j.eswa.2024.118456

[11] Nguyen, T., & Hoang, D. (2023). Real-time Threat Detection in UAVs Using Recurrent Neural Networks. Journal of Network and Computer Applications, 206, 103464. https://doi.org/10.1016/j.jnca.2023.103464

[12] Ahmad, M., & Rehman, S. (2022). Securing UAV Communications with Blockchain Technology: A Survey. Ad Hoc Networks, 136, 102953. https://doi.org/10.1016/j.adhoc.2022.102953

[13] Ghosh, R., & Banerjee, A. (2023). A Review of Digital Forensic Techniques for IoT and UAV Devices. Forensic Science International: Reports, 5, 100231. https://doi.org/10.1016/j.fsir.2023.100231

[14] Tan, Z., & Wang, H. (2024). Enhancing UAV Cybersecurity through Machine Learning: A Comparative Study. Information Sciences, 638, 423-445. https://doi.org/10.1016/j.ins.2024.02.017

[15] Choi, K., & Kim, Y. (2023). A Novel Approach to Drone Forensics Using Artificial Intelligence. Computers & Security, 118, 102634. https://doi.org/10.1016/j.cose.2023.102634

[16] Li, Z., & Zhao, J. (2022). Cybersecurity Threats and Solutions for UAV Networks. Journal of Communications and Networks, 24(4), 523-533. https://doi.org/10.23919/JCN.2022.000033

[17] Kumar, A., & Sharma, P. (2023). Integrating Deep Learning for Autonomous Drone Surveillance. Neural Computing and Applications, 35, 2035-2048. https://doi.org/10.1007/s00521-022-07342-7

[18] Evans, L., & Brown, D. (2024). Proactive Defense Strategies for UAVs Using Advanced Machine Learning Techniques. Journal of Information Security and Applications, 75, 103215. https://doi.org/10.1016/j.jisa.2024.103215

[19] Yadav, R., & Verma, K. (2023). Detection and Mitigation of Cyber Attacks in UAV Systems Using Deep Reinforcement Learning. Engineering Applications of Artificial Intelligence, 122, 105397. https://doi.org/10.1016/j.engappai.2023.105397

[20] Silva, J., & Mendes, A. (2022). Blockchain-Based Security Solutions for UAV Operations. Future Generation Computer Systems, 133, 191-203. https://doi.org/10.1016/j.future.2022.03.010

[21] Ibrahim, H., & Ali, F. (2023). An Efficient Anomaly Detection Framework for UAVs Using Machine Learning. IEEE Access, 11, 10356-10368. https://doi.org/10.1109/ACCESS.2023.3235432

[22] Wu, Y., & Zhang, T. (2024). A Comprehensive Survey on Drone Forensics and Security. Security and Privacy, 8(1), e179. https://doi.org/10.1002/spy2.179

[23] Chen, X., & Liu, Q. (2023). Implementing Machine Learning for Enhanced UAV Cybersecurity. Journal of Intelligent & Robotic Systems, 110, 255-270. https://doi.org/10.1007/s10846-022-01563-3

[24] Davis, S., & Wilson, R. (2022). Deep Learning Techniques for Proactive Cyber Defense in UAV Networks. Pattern Recognition Letters, 157, 1-10. https://doi.org/10.1016/j.patrec.2022.04.002