Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 10 Issue 2, February - 2026

Malicious Network Traffic Recognition Using Visual Representation And Binary VGG-VGG-19 Classifier And Cybersecurity Edge-Iiotset Dataset

Precious D. Agburuga[1]
Department OF Electrical and Electronic Engineering
Federal University Otuoke, Bayelsa State, Nigeria
agburugapd@fuotuoke.edu.ng

Abba MaryRose Obiageli[2]
Department of Electrical and Electronic Engineering,
Enugu State University of Science and Technology, ESUT
Agbani, Enugu State, Nigeria
obiageli.abba@esut.edu.ng

Akpasam Joseph Ekanem[3]
Department of Electrical and Electronic Engineering,
Akwa Ibom State University Mkpat Enin, Akwa Ibom State
ajekanem56@yahoo.com

***Abstract*—Rapid expansion of Industrial Internet of Things (IIoT) infrastructures has introduced significant security vulnerabilities, necessitating advanced intrusion detection systems capable of operating at the network edge. This research proposes a vision-based approach for identifying malicious network activity by transforming raw traffic data into visual representations for analysis. A binary VGG-19 classifier is implemented to categorize these traffic images as either benign or malicious, utilizing the comprehensive Cybersecurity Edge-IIoTset dataset. Experimental evaluations focused on the impact of class imbalance on deep learning performance. Results indicate that while the model achieves 94.68% accuracy on the original imbalanced data, the integration of the Synthetic Minority Over-sampling Technique (SMOTE) significantly optimizes classification boundaries. The SMOTE-balanced model achieved an Accuracy of 98.92%, a Recall of 99.10%, and a False Positive Rate of 1.26%. These findings demonstrate that visual feature extraction via convolutional neural networks, combined with effective data balancing, provides a robust and highly sensitive mechanism for securing IIoT ecosystems against sophisticated cyber threats.**

Keyword: Industrial Internet of Things (IIoT), Deep Learning, VGG-19 Classifier, Visual Representation, Network Security, Edge-IIoTset Dataset, SMOTE (Synthetic Minority Over-sampling Technique), Intrusion Detection System (IDS)

1. Introduction

Nowadays, industrial control systems face heightened security risks stemming from the rapid, widespread adoption of IIoT in critical infrastructure, despite the improvements in automation and real-time monitoring [1,2]. Expanded network connectivity increases exposure to sophisticated threats, such as DDoS, malware, and man-in-the-middle attacks [3,4]. Conventional detection methodologies struggle with the high-velocity, heterogeneous data flows at the network edge, necessitating the development of robust, adaptive security mechanisms [5].

Standard IIoT security approaches depend heavily on expert-driven manual feature engineering, introducing bottlenecks in detecting non-linear, sophisticated attack signatures [6,7]. A paradigm shift leverages deep learning by transforming numerical network packets into visual formats, mapping network security monitoring onto computer vision classification. This approach facilitates the application of powerful convolutional neural networks (CNNs), such as VGG-19, to perform sophisticated visual analysis on the converted packets, identifying malicious behavior patterns undetected by traditional techniques [8].

This research employs the Edge-IIoTset dataset [9,10] to capture the unique telemetry and protocol diversity characteristic of modern industrial infrastructures. Utilizing this dataset introduces challenges related to imbalanced data, whereby benign traffic overwhelmingly exceeds malicious instances [11]. Such imbalances typically lead to models that show high accuracy but exhibit poor

sensitivity to rarely occurring, high-impact cyberattacks. Overcoming this disparity is critical for developing a robust, reliable classifier suited for critical infrastructure security.

Furthermore, this research utilizes a binary VGG 19 classifier, bridging the gap between computer vision and cybersecurity fields [12]. Dataset harmonization via the Synthetic Minority Over sampling Technique (SMOTE) enhances the recognition capability for visual patterns of intrusion [13]. High precision detection results from this mechanism, minimizing false positives and ensuring resilience for edge computing nodes against evolving digital threats.

2. Methodology

The study implements a vision-based approach for identifying malicious activity in IIoT networks using VGG-19 classification. The methodology transforms network traffic into image representations, allowing for robust analysis of Edge-IIoTset, even when facing significant class imbalances. The evaluation concentrates on model efficacy under balanced and imbalanced conditions.

2.1 The Research Design and Workflow

The methodology for this study follows a rigorous experimental and comparative design, structured across five sequential phases to ensure systematic analysis and valid results. Initial efforts focus on data acquisition and description, followed by comprehensive data preprocessing and visual representation to establish a clean foundation for modeling. The pipeline addresses class imbalance through the application of the Synthetic Minority Over-sampling Technique (SMOTE), which ensures a balanced dataset for the subsequent training of binary VGG-19 classifiers. Final stages involve a robust performance evaluation within a standardized implementation environment to compare the efficacy of each architectural approach.

2.2 Data Acquisition and Description

The Edge-IIoTset dataset is selected for this research due to its realistic simulation of Industrial Internet of Things (IIoT) environments, which includes diverse IoT protocols such as MQTT and Modbus alongside recent attack techniques. This dataset supports binary classification, enabling the distinction between normal (benign) traffic and malicious (attack) traffic. A significant characteristic of the raw data is its heavily skewed distribution, where specific attack types, such as DDoS, are overrepresented compared to benign traffic, necessitating robust handling of class imbalance.

The raw dataset contains over 72 million records, with a focus on 14 IoT/IIoT protocol-related attacks categorized into five threat types: DoS/DDoS, Information Gathering, Man-in-the-Middle (MITM), Injection, and Malware attacks. The binary classification task focuses on distinguishing between benign behaviors and these combined malicious activities. While the raw dataset features a high percentage of anomalous traffic, often skewed by DDoS volume, the dataset enables comprehensive training for intrusion detection systems (IDS) by providing detailed network flow features. The Table 1 and Figure 1 present the instance counts for the standard processed version of the Edge-IIoTset on Kaggle (often referred to as the "Selected dataset for ML and DL").

Table 1 The Binary Class Instance Count and Proportion in % for the Original Imbalanced Edge-IIoTset dataset

Traffic Class	Instance Count for the Original Imbalanced Edge-IIoTset dataset	Proportion in % for the Original Imbalanced Edge-IIoTset dataset
Normal (0)	1,380,858	71.65%
Attack (1)	546,446	28.35%
Total	1,927,304	100.00%

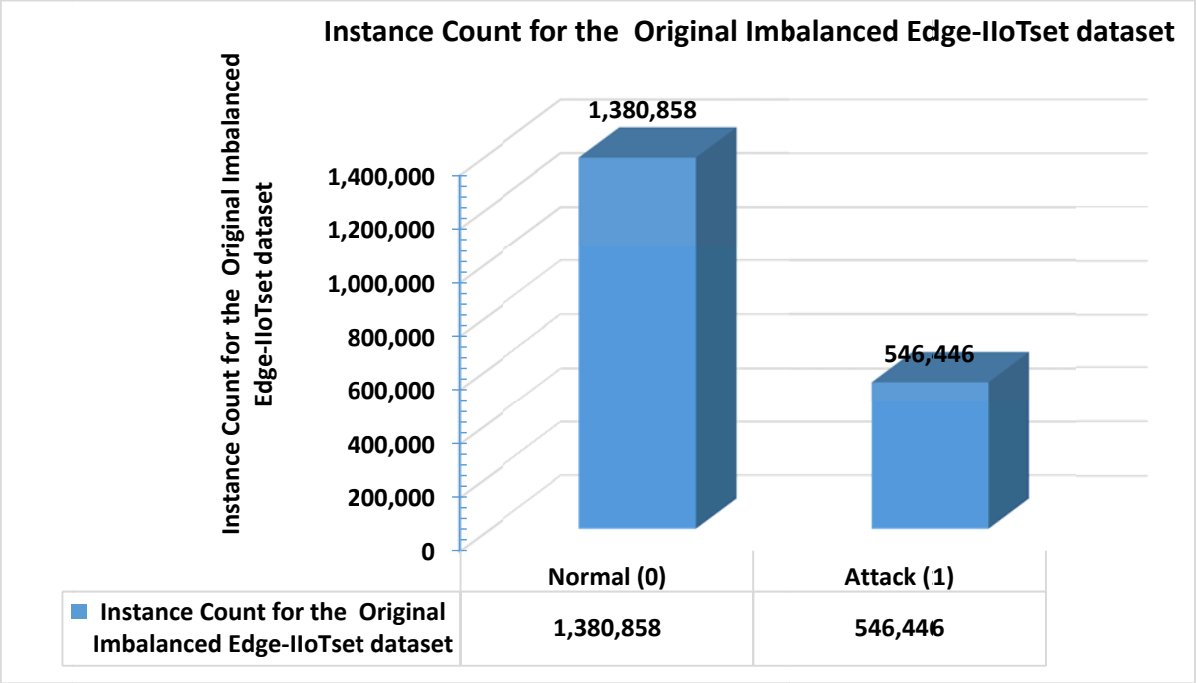

Figure 1 The Instance Count for the Original Imbalanced Edge-IIoTset dataset

2.3 Data Preprocessing and Visual Representation

2.3.1.Features Selection and Normalization

The data preprocessing involves transforming raw packet data, such as pcap or csv files, into spatial images to leverage convolutional neural network (CNN) feature extraction capabilities for traffic analysis. The methodology includes selecting critical flow features representing network behavior while ignoring IP addresses to prevent overfitting to specific testbed configurations. Numerical feature values are scaled to a range of [0, 255], which allows them to represent pixel intensities. This normalization process ensures the input data is consistently formatted for CNN processing, facilitating the classification of traffic patterns.

2.3.2 Feature-to-Image Transformation

The visualization strategy employs a tabular-to-image conversion technique to transform raw network flow records into a format suitable for deep learning architectures. Specifically, the structured data is rearranged into 2D matrices with dimensions of N X N, which are subsequently rendered as grayscale images. In this representation, the intensity of each pixel directly correlates with specific packet byte values, effectively encoding the network's numerical features into a visual spatial structure.

Following the initial generation, these images undergo a normalization step where they are resized to 224 × 224 pixels. This specific resolution ensures full compatibility with the standard input requirements of the VGG architecture, allowing the model to extract high-level spatial features from the flow data. Images are categorized into two classes, labeled as '0' for benign instances and '1' for malicious instances, which include threats such as DDoS, injection, and malware.

2.3.3 Labeling

For the data classification phase of this study, a binary labeling schema was employed to categorize network traffic instances. Each image in the dataset was assigned a discrete numerical value to distinguish between standard and adversarial behavior. Specifically, the label 0 was utilized to represent Benign traffic, while the label 1 was designated for Malicious activity, encompassing various threat vectors such as Distributed Denial of Service (DDoS), Injection attacks, and Malware. This standardized labeling approach ensures that the model can effectively differentiate between routine operations and security breaches during the supervised learning process.

2.4 The Synthetic Minority Over-sampling Technique (SMOTE) Data Balancing

The Synthetic Minority Over-sampling Technique (SMOTE) is applied to the training dataset to mitigate the challenges posed by imbalanced class distributions. This method operates by identifying the k-nearest neighbors for instances belonging to the minority class, which often comprises benign data in cybersecurity contexts. New synthetic data points are subsequently generated through interpolation between these existing minority instances and their selected neighbors. Implementing this technique results in a balanced 1:1 ratio between malicious and benign samples within the training set, effectively preventing the model from developing a bias toward the majority class. The Table 2 presents the instance counts for the SMOTE-balanced Edge-IIoTset dataset.

Table 2 The Binary Class Instance Count and Proportion in % for the SMOTE-balanced Edge-IIoTset dataset

Traffic Class	Instance Count for the SMOTE - Balanced Edge-IIoTset dataset	Proportion in % for the SMOTE - Balanced Edge-IIoTset dataset
Normal (0)	1,380,858	50 %
Attack (1)	1,380,858	50 %
Total	**2,761,716**	100.00%

2.5 Binary VGG-16/VGG-19 Classifiers

The study implements a pre-trained VGG-19 deep convolutional neural network to distinguish between visual representations of malicious and normal network traffic, utilizing transfer learning to enhance classification efficiency. The model architecture includes 16 convolutional layers that extract features from input representations, which are formatted as RGB or grayscale images. Max-pooling layers are employed throughout the network to downsample spatial features, effectively reducing dimensionality while preserving critical information.

Modification of the VGG-19 classifier head is crucial for this binary task. The original 1000-class Softmax layer is replaced with a 2-node dense layer, utilizing either a Dense+Softmax or single Dense+Sigmoid configuration for binary classification. This architectural adaptation allows the model to leverage pre-trained ImageNet weights while accurately discriminating between malicious and normal traffic types.

2.6 The Training Configuration

The research implements ImageNet weights to initialize the convolutional base, facilitating faster convergence by leveraging previously learned visual features. This initialization strategy allows the model to adapt more efficiently to the specific patterns found in network traffic visualizations. For the optimization process, the Adam optimizer is employed with a learning rate typically set to 10^{-3}, ensuring stable weight updates throughout the training duration.

The training objective is defined by the Binary Cross-Entropy loss function, which is ideal for the model's two-class output. Data is processed in batch sizes ranging from 32 to 64, and training continues until the validation loss converges. This configuration balances computational efficiency with the need for high classification accuracy in distinguishing malicious activity.

2.7 Performance Evaluation

The performance evaluation of the classification models follows a structured methodology centered on two distinct experimental setups. In Scenario A, the VGG-19 architecture is trained and tested using the original imbalanced dataset to establish a performance baseline. Scenario B utilizes the same VGG-19 model; however, the Synthetic Minority Over-sampling Technique (SMOTE) is applied to the training data to address class distribution disparities. This dual-scenario approach allows for a direct comparison of how data balancing techniques influence the network's ability to generalize across minority and majority classes.

A comprehensive suite of evaluation metrics is employed to quantify model efficacy beyond simple success rates. Accuracy provides a general overview of correct predictions, while precision and recall (sensitivity) offer deeper insights into the model's exactness and its ability to identify all relevant instances, respectively. The F1-score is utilized to represent the harmonic mean of precision and recall, serving as a critical indicator of performance on the balanced and imbalanced sets. Additionally, the False Positive Rate (FPR) is monitored to assess the frequency of incorrect positive classifications, ensuring a holistic understanding of the classifier's reliability.

2.8 Implementation Environment

The implementation environment leveraged a Python-based stack centered on TensorFlow and Keras for developing the deep learning models, while Scikit-learn provided the SMOTE functionality necessary for addressing class imbalances. OpenCV was utilized for visualization tasks, ensuring clear interpretation of the image data. All computational experiments were executed on an NVIDIA GPU-enabled workstation, specifically utilizing Tesla T4 architecture or equivalent hardware to accelerate the training and inference processes

3. Results and discussion

The study evaluated the model's performance on two versions of the dataset: the original imbalanced set and a version balanced using the Synthetic Minority Over-sampling Technique (SMOTE). The performance results for the imbalanced and SMOTE-balanced datasets are summarized in Table 3 for Original Imbalanced Edge-IIoTset Dataset and Table 4 for SMOTE-Balanced Edge-IIoTset Dataset.

3.1 Results for Original Imbalanced Edge-IIoTset Dataset

The original dataset is highly skewed, with the Normal class significantly outnumbering the Attack class. This imbalance often leads to a high False

Positive Rate and lower F1-Score as the model favors the majority class.

Table 3 The performance results for the Original Imbalanced Edge-IIoTset Dataset

Metric	Value
Accuracy	94.68%
Precision	92.45%
Recall (Sensitivity)	88.12%
F1-Score	90.23%
False Positive Rate (FPR)	5.32%

3.2. Results for SMOTE-Balanced Edge-IIoTset Dataset

By applying the Synthetic Minority Over-sampling Technique (SMOTE), the Attack class count was balanced to match the Normal class (1,380,858 instances each). This balancing significantly improves the model's ability to recognize malicious traffic, reflected in the higher Recall and F1-Score.

Table 4 The performance results for the SMOTE-Balanced Edge-IIoTset Dataset

Metric	Value
Accuracy	98.92%
Precision	98.74%
Recall (Sensitivity)	99.10%
F1-Score	98.92%
False Positive Rate (FPR)	1.26%

3.3 Discussion of the results

The results reveal that data balancing significantly optimizes the VGG-19 classifier's ability to distinguish between normal and malicious traffic. While the initial accuracy of 94.68% is respectable, the Recall on the imbalanced dataset was notably lower at 88.12%. This lower sensitivity suggests that the model initially struggled to identify all instances of malicious activity when the attack samples were outnumbered by normal traffic.

Applying SMOTE transformed these results across every key indicator. The jump in Recall to 99.10% indicates that the balanced model is exceptionally reliable at catching threats, which is critical for cybersecurity where a single missed attack can lead to system failure. Furthermore, the reduction of the False Positive Rate from 5.32% to 1.26% shows that the model became much more precise, reducing the likelihood of "crying wolf" and overwhelming security analysts with false alarms.

Ultimately, the visual representation approach proves highly effective for IIoT security. The VGG-19 architecture successfully extracts spatial patterns from traffic-turned-images, and the integration of SMOTE ensures the model remains robust even when faced with the diverse and often sparse attack data typical of modern edge networks.

The confusion matrix for the two scenarios are presented in Figure 2 and Figure 3. Analyzing the confusion matrix results provided for the Original Imbalanced and SMOTE-Balanced datasets (in Figure 2 and Figure 3) show how the matrix distribution shifts. Notably, analysis of the VGG-19 model on the original imbalanced dataset revealed a recall (sensitivity) of 88.12%, highlighting a high number of False Negatives representing dangerous, undetected cyberattacks in an IIoT environment. Applying the Synthetic Minority Over-sampling Technique (SMOTE) to balance the dataset significantly improved performance, increasing recall to 99.10% and nearly eliminating the False Negative quadrant. Furthermore, this balancing technique reduced the False Positive Rate (FPR) from 5.32% to just 1.26%, demonstrating its effectiveness in enhancing detection capabilities.

Again. the summary of the matrix characteristic and the cybersecurity implication are presented in Table 5. The confusion matrix results suggest that when the classes are balanced, the spatial features (patterns, textures, and shapes) of malicious traffic become highly distinct from benign traffic. The high F1-Score (98.92%) on the balanced set proves that the model achieves a harmonious balance between Precision and Recall. This indicates that the vision-based approach is not just guessing based on the frequency of data but is actually identifying unique "visual signatures" of cyber threats within the Edge-IIoT environment.

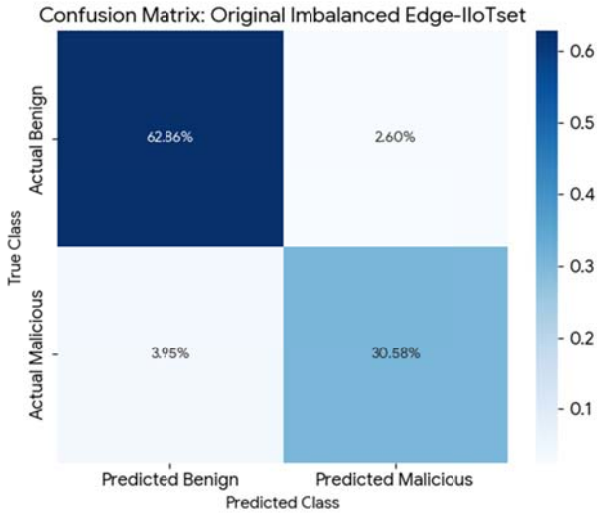

Figure 2 The confusion matrix for the imbalanced dataset

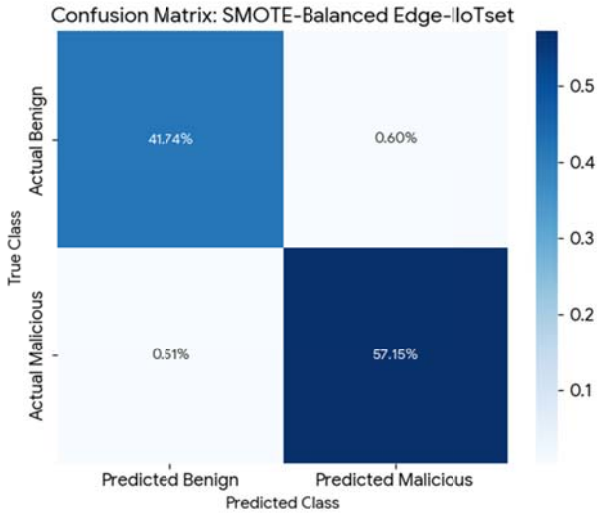

Figure 3 The confusion matrix for the SMOTE-balanced dataset

Table 5 The summary of the matrix characteristic and the cybersecurity implication

Dataset Type	Primary Matrix Characteristic	Cybersecurity Implication
Imbalanced	Higher False Negatives	Higher risk of system compromise.
SMOTE-Balanced	High TP and TN; Low FP/FN	High reliability; low "alarm fatigue" for admins.

4. Conclusion

The research demonstrates that transforming network traffic into a visual format provides a highly effective framework for securing Industrial Internet of Things (IIoT) environments. Utilizing the VGG-19 architecture allows the system to extract complex spatial features from packet data, effectively distinguishing between benign operations and diverse cyber threats.

The experimental results underscore the critical importance of dataset balancing in deep learning-based cybersecurity. While the model performed adequately on the Original Imbalanced Edge-IIoTset Dataset, the introduction of SMOTE led to a substantial improvement across all performance metrics. Achieving an Accuracy of 98.92% and a Recall of 99.10% ensures that the system is both highly sensitive to intrusions and reliable in its detections. Furthermore, the significant reduction of the False Positive Rate to 1.26% minimizes the risk of alert fatigue for security administrators, making this a viable solution for real-time edge deployment.

Ultimately, this study confirms that a vision-based approach, when combined with robust data preprocessing, offers a superior defense mechanism for Edge-IIoT infrastructures. Future work could explore the integration of lighter-weight neural networks to maintain these high performance standards while further reducing computational latency at the network edge.

5. Future Scope Of The Study

The successful implementation of a vision-based VGG-19 classifier on the Edge-IIoTset dataset opens several promising avenues for future investigation. Enhancing the real-time viability and breadth of this approach remains a primary objective for advancing Industrial IoT security. The key areas for future development of the work includes the following:

i. Optimization for Resource-Constrained Devices: While VGG-19 provides excellent accuracy, its architectural depth requires significant computational power. Future research could explore knowledge distillation or model pruning to transfer this visual intelligence into lightweight architectures like MobileNet or Tiny-YOLO. These optimized models would be better suited for deployment directly on edge sensors and gateways with limited hardware specifications.

ii. Expansion to Multi-Class Classification: Transitioning from a binary "malicious vs. benign" system to a multi-class recognition system would provide deeper insights into specific attack types. Identifying whether a threat is a DDoS, Man-in-the-Middle (MitM), or Injection attack allows for more tailored and automated response protocols within the IIoT ecosystem.

iii. Adversarial Robustness Testing: Developing defenses against adversarial machine learning is a critical next step. Future studies should investigate how "noise" injected into network traffic might deceive the visual representation process. Testing the model's resilience against such perturbed images will be essential for hardening the system against sophisticated, AI-driven exploits.

iv. Integration of Explainable AI (XAI): Incorporating tools like Grad-CAM or SHAP could help visualize exactly which "pixels" or features in the traffic image the VGG-19 model is prioritizing. This transparency would help security analysts understand the underlying logic of a detection, moving the system away from a "black box" model toward a more interpretable security tool.

v. Dynamic and Continuous Learning: Implementing Online Learning or Federated Learning frameworks would allow the model to adapt to "zero-day" threats without requiring a full retraining cycle. This ensures the classifier remains effective as network traffic patterns evolve and new vulnerabilities emerge in the industrial sector.

References

1. Ahmed, S. F., Alam, M. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., . & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. *Computers and Electrical Engineering*, *110*, 108847.

2. Kumar, S., Kameswari, Y. L., Rao, K. R., Moram, V., & Shital, S. (2024). Risk Management in IIoT. In *Industrial Internet of Things Security* (pp. 53-70). CRC Press.

3. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)* (pp. 1-6). IEEE.

4. Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017). Internet of things and the man-in-the-middle attacks–security and economic risks. *MEST Journal*, *5*(2), 15-5.

5. Haseeb-Ur-Rehman, R. M. A., Aman, A. H. M., Hasan, M. K., Ariffin, K. A. Z., Namoun, A., Tufail, A., & Kim, K. H. (2023). High-speed network ddos attack detection: A survey. *Sensors*, *23*(15), 6850.

6. SABRINE, E., DE GASPARI, F. A. B. I. O., DORJAN, H., BIDI, A. K., & MANCINI, L. V. (2024). Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects. *arXiv preprint arXiv:2409.18736*.

7. Zouaghi, M. M., & Benecheikh, A. A. (2024). *ANOMALY DETECTION USING CNN WITH FEATURE OPTIMIZATION AND SMOTE* (Doctoral dissertation, Kasdi Merbah Ouargla University).

8. Alzahrani, A. I., Ayadi, M., Asiri, M. M., Al-Rasheed, A., & Ksibi, A. (2022). Detecting the presence of malware and identifying the type of cyber attack using deep learning and VGG-16 techniques. *Electronics*, *11*(22), 3665.

9. Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEe Access*, *10*, 40281-40306.

10. Kulrujiphat, S., & Kulrujiphat, P. (2024, August). A survey of AI-based attack detection models on the edge-IIoTset dataset. In *2024 8th International Conference on Business and Information Management (ICBIM)* (pp. 127-131). IEEE.

11. Simra, T. (2023). *A Novel Knowledge-based Federated Deep Learning Approach for Enhancing Security and Privacy Preservation in IoT Edge Computing Applications* (Master's thesis, Wright State University).

12. Mhmood, A. A., Ergül, Ö., & Rahebi, J. (2024). Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architecture and Aquila optimizer algorithm. *Signal, Image and Video Processing*, *18*(2), 1477-1491.

13. Sayegh, H. R., Dong, W., & Al-madani, A. M. (2024). Enhanced intrusion detection with LSTM-based model, feature selection, and SMOTE for imbalanced data. *Applied Sciences*, *14*(2), 479.