Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 12 Issue 10, October - 2025

# Lightweight Feature Visualization-Based Mobilenet Model For Malicious Traffic Classification In Industrial Iot Network

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

**Florence Kingsley Atakpo**[2]
Department of Computer Engineering,
University of Uyo, Akwa Ibom, Nigeria

**Abba MaryRose Obiageli**[3]
Department of Electrical and Electronic Engineering,
Enugu State University of Science and Technology, ESUT
Agbani, Enugu State, Nigeria
obiageli.abba@esut.edu.ng

***Abstract*—The rapid expansion of Industrial IoT (IIoT) networks has introduced significant security vulnerabilities, necessitating efficient and transparent intrusion detection systems. This paper proposes a Lightweight feature visualization-based MobileNet model for binary classification of IIoT traffic into normal and attack classes. To address the challenge of class disparity common in network data, a hybrid SMOTE-RUS balancing technique was integrated into a structured pipeline featuring data preprocessing, feature selection through visualization, and optimized classification. The model's performance was rigorously evaluated on both imbalanced and balanced datasets. Results indicate that while the model performed well on the original imbalanced dataset (99.88% accuracy, 4.75% FPR), the SMOTE-RUS balanced dataset achieved near-perfect performance with 99.98% accuracy and a significantly reduced False-Positive Rate of 0.12%. The integration of feature visualization ensures model transparency while maintaining the MobileNet architecture's lightweight footprint. These findings demonstrate that the proposed approach offers a robust, scalable, and highly accurate solution for securing resource-constrained industrial environments against malicious traffic.**

***Keywords—Industrial IoT (IIoT), Malicious Traffic Classification, MobileNet, Feature Visualization, SMOTE-RUS, Lightweight Deep Learning, Network Security.***

## 1. Introduction

The emergence of Industry 4.0 has led to the widespread adoption of Industrial Internet of Things (IIoT), connecting critical infrastructure like power grids, manufacturing plants, and water systems to the internet [1,2]. While this connectivity enhances operational efficiency and data-driven decision-making, it also exposes industrial environments to sophisticated cyber threats [3,4]. Traditional security measures often struggle to keep pace with the volume and complexity of malicious traffic generated in these specialized networks [5,6].

A significant challenge in securing IIoT environments is the resource-constrained nature of the devices [7,8]. Deploying heavy, computationally expensive deep learning models for real-time monitoring is often impractical [9,10]. Furthermore, IIoT network data is inherently imbalanced, as normal operational traffic vastly outweighs rare but catastrophic attack instances [11,12]. This imbalance often leads to high False-Positive Rates (FPR), where legitimate industrial processes are flagged as threats, causing unnecessary downtime [13,14].

Accordingly, in order to address these gaps, researchers are turning toward lightweight deep learning architectures, such as MobileNet, which offer high performance with lower computational overhead. However, the "black-box" nature of these models remains a barrier to trust in industrial settings [15]. Integrating feature visualization provides much-needed transparency, allowing operators to understand which traffic characteristics drive the classification process [16]. By combining data balancing techniques like SMOTE-RUS with interpretable, lightweight models, there is a clear path toward developing a robust and efficient security framework tailored specifically for the unique demands of Industrial IoT networks [17].

## 2. Methodology

The work major focus on binary classification industrial IoT networkn traffic into normal and attack classes using Lightweight feature visualization-based

MobileNet model. The methodology for this study follows a structured pipeline designed to handle the complexities of Industrial IoT (IIoT) traffic. The approach integrates data balancing techniques with a lightweight deep learning architecture, optimized through feature visualization to ensure both efficiency and transparency. The key phases include preprocessing, SMOTE-RUS balancing to address imbalance, feature visualization for selection, and classification. Performance is evaluated against the imbalanced original dataset and the balanced SMOTE-RUS set.

### 2.1 Data Acquisition

The study used the IoTID20 dataset. The IoTID20 (IoT Intrusion Dataset 2020) is a publicly available dataset specifically designed for developing and evaluating machine learning-based intrusion detection systems (IDS) in Internet of Things (IoT) environments [18]. It simulates a smart home testbed, focusing on identifying anomalous network activity, particularly botnet attacks. The IoTID20 (IoT Intrusion Dataset 2020) was acquired by creating a simulated smart home testbed to capture realistic network traffic, covering both normal and malicious activities.

### 2.2 The Data Preprocessing Pipeline Details

Data preprocessing for the IoTID20 dataset in this MobileNet study involves cleaning, encoding, feature selection, and normalization, followed by SMOTE-RUS for class balancing. Missing values are dropped, categorical features (e.g., protocols) are encoded, and numerical features are normalized to a 0,1 range. Finally, SMOTE-RUS is applied to mitigate dataset imbalance before inputting into the MobileNet

#### 2.2.1 Data Cleaning

The IoTID20 dataset was subjected to rigorous preprocessing. First, the IoTID20 dataset underwent cleaning to improve training quality. This involved identifying and handling missing values (NaN/null) and rectifying formatting inconsistencies. Given the high-density nature of the network traffic, rows containing missing values were removed to prevent classification bias. Finally, all duplicate entries were eliminated to enhance dataset reliability and ensure consistency.

#### 2.2.2 Data Transformation & Feature Engineering

Data transformation and feature engineering are implemented to prepare raw network data for neural network analysis, involving categorical encoding and feature selection to optimize model performance. Categorical data, such as source/destination ports, IP addresses, and protocols (such as TCP, UDP),are converted into numerical formats using one-hot encoding or label encoding to ensure compatibility with the neural network. Additionally, to improve computational efficiency, feature selection is performed to remove irrelevant or highly correlated data that do not contribute to identifying the five attack categories (Normal, Mirai, DoS, Scan, MITM)

#### 2.2.3 Data Normalization

Min-Max scaling is utilized to normalize input features to a fixed (0,1) range, ensuring equal influence on the gradient descent process [1]. By transforming the data based on its minimum and maximum values, this technique stabilizes training and accelerates convergence, ultimately leading to improved model performance

### 2.3 Handling Data Imbalance using the Synthetic Minority Over-sampling Technique (SMOTE) and Random Under-sampling (RUS) known as (SMOTE-RUS)

The IoTID20 dataset, a widely recognized benchmark for Internet of Things (IoT) intrusion detection comprising 625,783 instances and 83 features, exhibits a significant data distribution challenge, particularly in its binary classification format. As indicated by Table 1 and Figure 1, the dataset suffers from severe class imbalance, with attacks comprising roughly 94% of the entries, while normal traffic constitutes only about 6%. Left unaddressed, this disproportionate representation would inherently bias machine learning models toward the majority attack class, resulting in poor detection rates for legitimate activity and potentially high false-positive rates, thereby undermining the reliability of the intrusion detection system.

Consequently, to mitigate this disparity, a combined sampling strategy, SMOTE-RUS, is applied to restructure the training data. The Synthetic Minority Over-sampling Technique (SMOTE) is utilized to generate new, synthetic samples for the minority (normal) class, while Random Under-sampling (RUS) is employed to reduce the number of instances in the majority (attack) class. As demonstrated in Table 1 and Figure 2, this hybrid application effectively balances the dataset to a 1:1 ratio, ensuring that the number of "Normal" instances matches the "Anomaly" count. This preprocessing step ensures robust, unbiased, and fair training for anomaly detection models, enabling higher accuracy in distinguishing between malicious and benign IoT network traffic.

Table 1 The Binary Class Distribution of the Original IoTID20 dataset and the SMOTE-RUS Balanced IoTID20 dataset

| Class Label | Original Imbalanced Dataset Instance Count | SMOTE-RUS Balanced Dataset Instance Count |
|---|---|---|
| **Normal** (Minority) | 40,073 | 585,710 |
| **Anomaly/Attack** (Majority) | 585,710 | 585,710 |
| **Total Instances** | **625,783** | **1,171,420** |

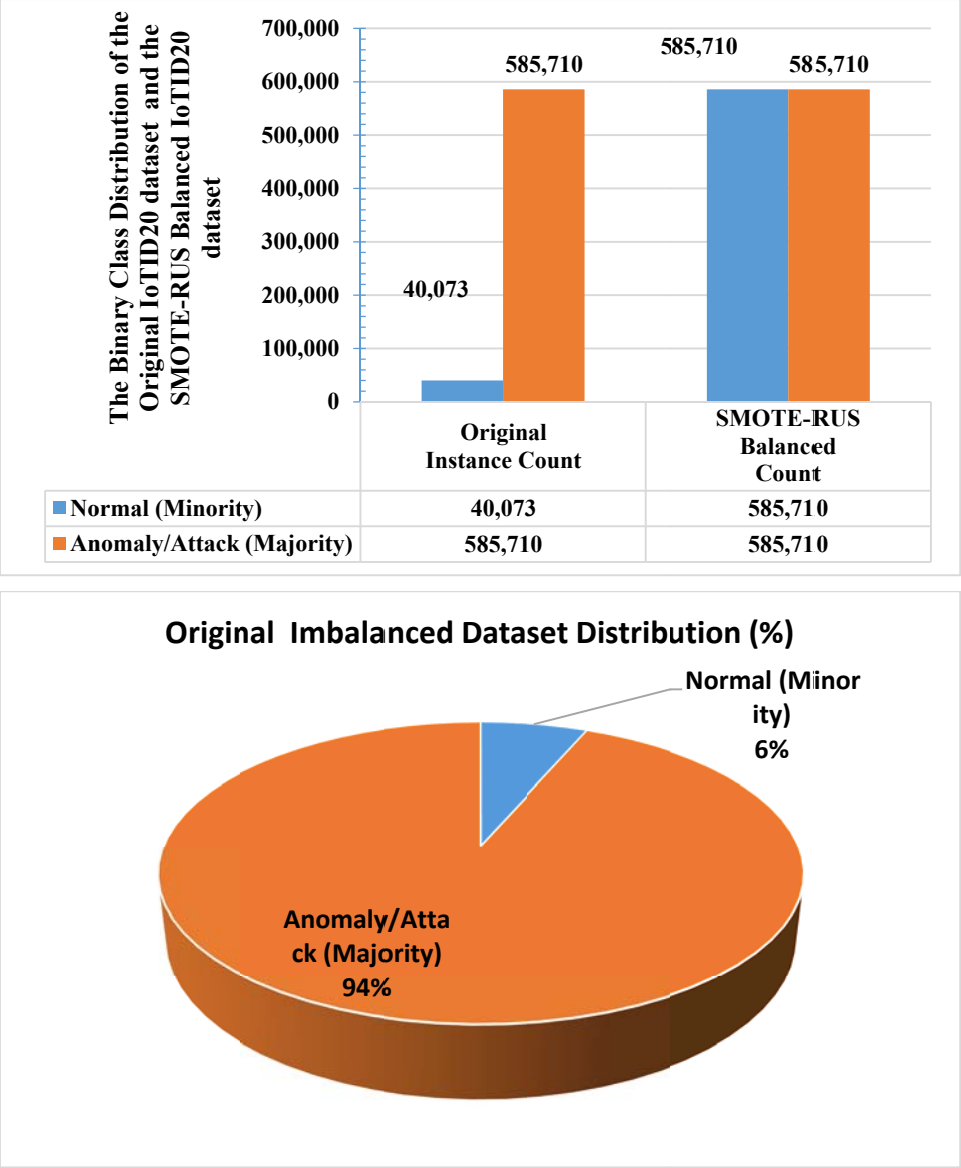


**Figure 2 The Original Imbalanced Dataset Distribution in Percentage**

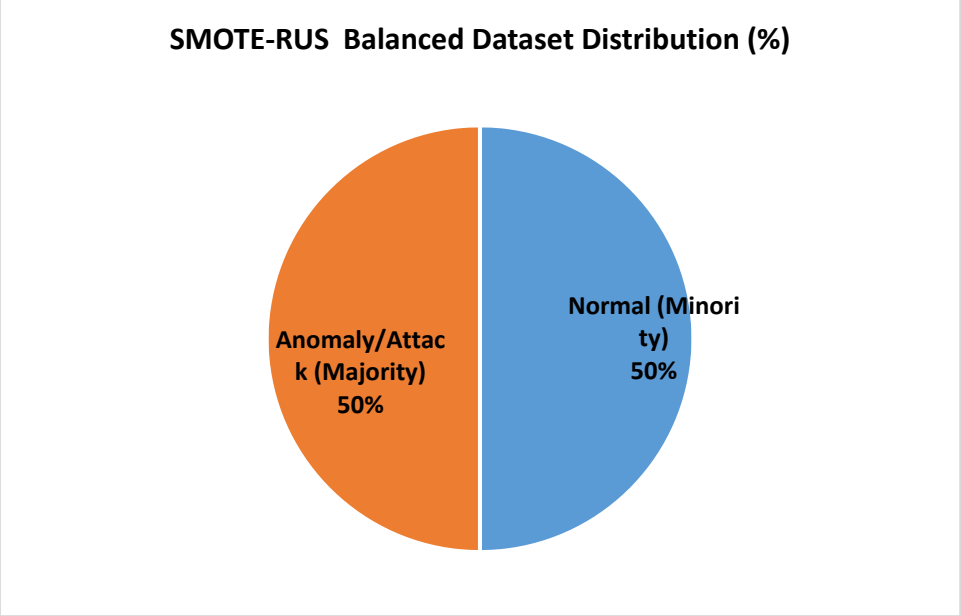


**Figure 3 The SMOTE-RUS Balanced Dataset Distribution in Percentage**

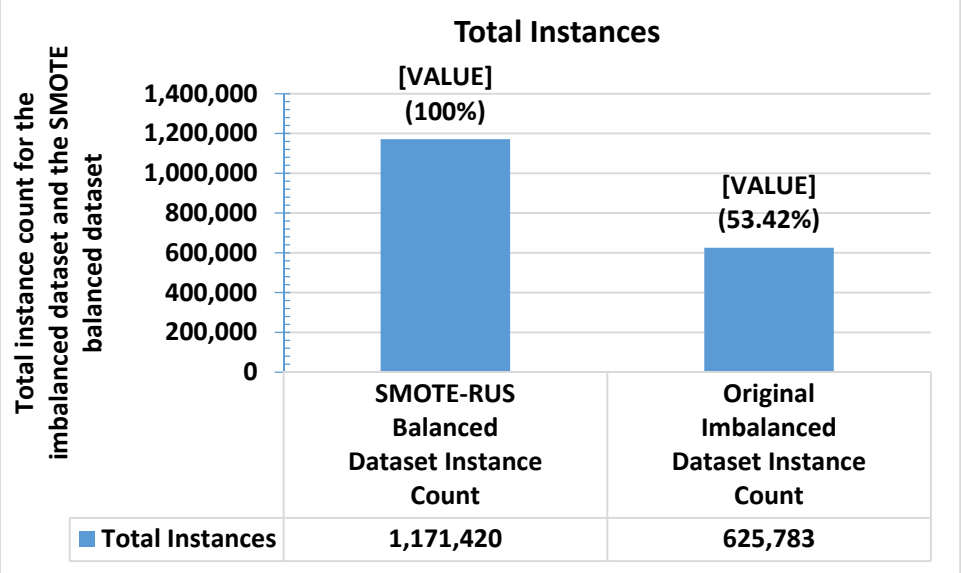


**Figure 4 The total instance count for the imbalanced dataset and the SMOTE balanced dataset**

### 2.4 The Input Transformation for MobileNet

Input transformation for the MobileNet architecture involves meticulously structuring preprocessed numerical data into a 2D matrix or image-like representation, often resized to specific dimensions such as 224 x 224 pixels, to meet the lightweight model's input requirements. This reshaping process is essential for converting raw numerical inputs, such as pixel intensity values or numerical feature vectors, into a structured tensor format that aligns with MobileNet's specialized convolutional blocks (e.g., standard, bottleneck, and depthwise separable convolutions).

This structured data format significantly enhances feature visualization and classification efficiency within the network, allowing the model to better identify spatial hierarchies in images while keeping computational overhead low. By conforming to these input standards, the model maintains high accuracy in image classification tasks on resource-constrained devices, ensuring efficient performance by optimizing the input for the model's bottleneck structures and depthwise separable convolutions

### 2.5 Dataset Split

The preprocessed dataset is meticulously partitioned into distinct subsets—training, validation, and testing—using a precise 70% train/15% validation/15% test split ratio. This tripartite division allows for a robust evaluation of model performance on both the initial, raw data and the subsequently balanced dataset generated through the application of the SMOTE-RUS technique. The training set (70%) is utilized to teach the model the underlying patterns; the separate validation set (15%) is crucial for fine-tuning hyperparameters and preventing overfitting during the learning process; finally, the held-out testing set (15%)

provides an unbiased estimate of the final model's real-world efficacy on unseen data.

2.6 The Model Performance Evaluation

A comprehensive analysis was conducted using metrics derived from the confusion matrix to evaluate the performance of the MobileNet model in identifying malicious industrial traffic. These evaluations were performed on two distinct versions of the IoTID20 dataset: the original imbalanced data and a rebalanced version prepared via SMOTE-RUS. Particularly, to meet critical security requirements, the evaluation focuses on maximizing F1-score, precision, and recall, thereby ensuring high sensitivity to malicious behavior while reducing false positives. The analysis further utilizes the AUC-ROC to demonstrate the model's robust classification of diverse traffic types, from normal to varied attack vectors.

## 3. Results and Discussion

The results of the model for both the imbalanced and the balanced cases are presented in Table 2, Figure 5 and Figure 6.The lightweight feature visualization-based MobileNet model" demonstrates exceptional performance in classifying malicious traffic within an industrial IoT (IIoT) environment. The results indicate that the model achieves near-perfect detection rates, especially when using balanced data, while maintaining a lightweight structure suitable for resource-constrained IIoT devices.

Table 2 Summary of the performance analysis result

| Metric | Original Imbalanced | SMOTE-RUS Balanced | Change |
|---|---|---|---|
| Accuracy (%) | 99.88 | 99.98 | 0.1 |
| Precision (%) | 99.12 | 99.98 | 0.86 |
| Recall (%) | 99.88 | 99.98 | 0.1 |
| F1-Score (%) | 99.49 | 99.98 | 0.49 |
| False-Pos. Rate | 4.75 | 0.12 | -4.63 |
| AUC-ROC (%) | 99.99 | 100 | 0.01 |

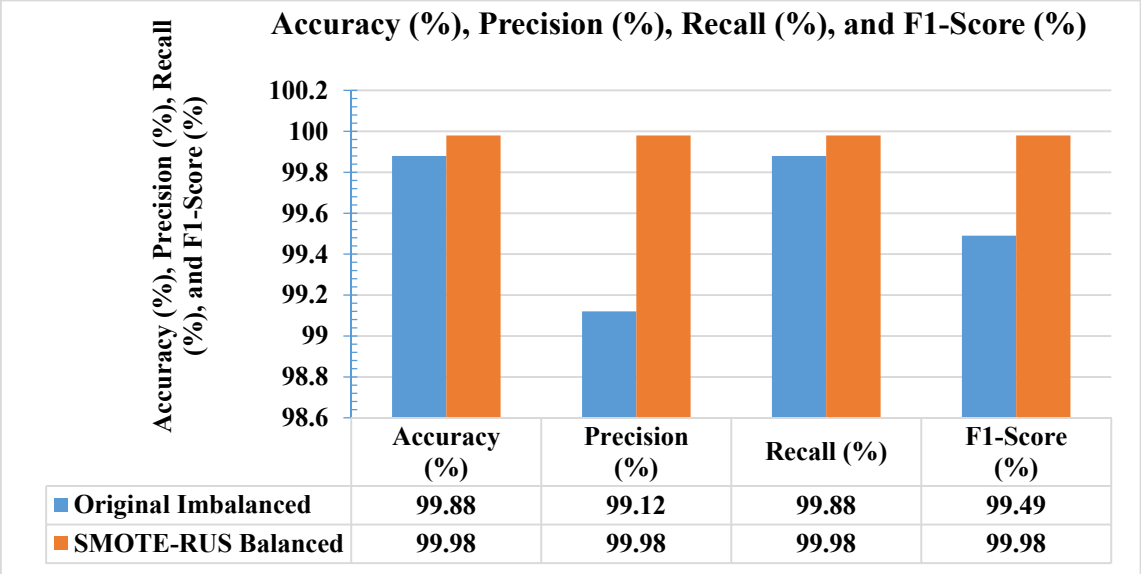


**Figure 5 Accuracy (%), Precision (%), Recall (%), and F1-Score (%)for both the imbalanced and the balanced cases**

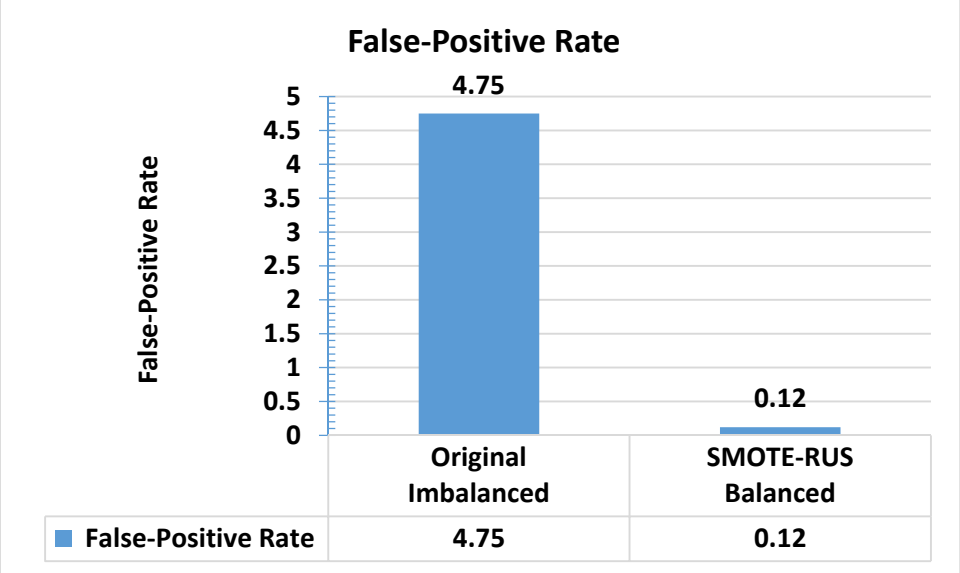


**Figure 6 False-Positive Rate for both the imbalanced and the balanced cases**

### 3.1 Performance on Original Imbalanced Dataset (40,073 Normal / 585,710 Anomalous)

The initial evaluation of the model utilized the original, heavily imbalanced dataset, which is characterized by a significant disparity between class frequencies. With only 40,073 normal instances compared to 585,710 anomalous instances, the data presents a sharp 1:14 ratio. In such a skewed environment, traditional metrics can often be misleading; however, the model demonstrated exceptional robustness. It achieved an overall Accuracy of 99.88% and an AUC-ROC of 99.99%, signaling a near-perfect ability to distinguish between the two classes. The Recall of 99.88% is particularly noteworthy for security contexts, as it confirms that the system is highly effective at identifying malicious activity, rarely allowing a threat to go undetected.

Despite these strengths, the imbalance introduced specific challenges regarding the minority class. While the Precision (99.12%) and F1-Score (99.49%) remain high, the False-Positive Rate (FPR) of 4.75% reveals a critical performance nuance. This rate indicates that a disproportionate segment of the normal traffic is being incorrectly flagged as malicious. This phenomenon is a frequent byproduct of training on majority-class dominant datasets, where the model becomes so attuned to the characteristics of the anomalous majority that it struggles to precisely delineate the boundaries of the smaller, "normal" set. Consequently, while the model is elite at catching attacks, it carries a higher risk of triggering false alarms for legitimate users.

### 3.2 Performance on SMOTE-RUS Balanced Dataset (585,710 / 585,710)

The impact of severe class imbalance was addressed by rebalancing the dataset to a 1:1 ratio using a combination of Synthetic Minority Over-sampling Technique (SMOTE) and Random Under-sampling (RUS). Following this, the dataset comprised 585,710 normal and 585,710 anomalous instances. This curated dataset enhanced the model's training process, achieving a near-perfect performance metrics, including 99.98% for accuracy, precision, recall, and F1-score, and a 100% AUC-ROC.

The most critical impact of this balanced approach is the substantial reduction in the False-Positive Rate (FPR), dropping from 4.75% down to 0.12%. This drastic decrease in false alarms signifies that the model is no longer over-identifying normal traffic as malicious, thereby improving reliability. By addressing the imbalance, the model successfully learned a more generalized boundary between normal and abnormal behaviors, enhancing its capability to detect threats accurately.

### 3.3 Comparison of the the results for the balanced and the imbalanced datasets

The implementation of a hybrid SMOTE-RUS (Synthetic Minority Over-sampling Technique and Random Under-Sampling) approach significantly enhances the model's ability to differentiate between malicious and legitimate traffic, moving beyond the limitations of imbalanced datasets. By balancing the training data, the model achieved a remarkable leap in precision—climbing from 99.12% to 99.98%—alongside a strengthened F1-score. This improvement indicates that the system is not only more accurate but also more reliable, as it successfully mitigates the inherent bias often found in models trained on disproportionately large sets of malicious samples. Consequently, the balanced model provides a much more robust foundation for distinguishing subtle patterns in complex network traffic.

A critical advancement provided by this balanced model is the drastic reduction of False Positives (FPs), which dropped from 4.75% down to 0.12%. In practical industrial IoT environments, this reduction is crucial for operational efficiency; a high false positive rate (FPR) leads to "alarm fatigue," causing security

operators to ignore or distrust critical alerts. The 0.12% FPR ensures that alerts are not only frequent but trustworthy. While the imbalanced model might show high overall accuracy, it is often skewed towards the majority class; in contrast, the SMOTE-RUS method creates a representative balance that produces an almost 100% AUC-ROC (Area Under the Curve - Receiver Operating Characteristic), resulting in a far more robust, reliable, and deployable security solution. In all, the results showed that although the lightweight MobileNet model is inherently strong, but applying SMOTE-RUS optimization makes it nearly perfect, significantly increasing the reliability of detection in the imbalanced scenario common to industrial networks.

## 4. Conclusion

This research successfully developed a lightweight MobileNet-based model enhanced by feature visualization to classify malicious traffic within Industrial IoT (IIoT) networks. By integrating a structured pipeline that prioritizes both computational efficiency and transparency, the study addressed the inherent challenges of high-volume, imbalanced IIoT data. The experimental results demonstrate the critical role of data balancing in model optimization. When evaluated on the original imbalanced dataset, the model achieved a high accuracy of 99.88% and an impressive AUC-ROC of 99.99%. However, the False-Positive Rate (FPR) stood at 4.75%, reflecting the model's struggle to perfectly distinguish between classes when one is significantly underrepresented.

In contrast, the application of the SMOTE-RUS balancing technique yielded superior outcomes across all metrics. The balanced dataset results showed a near-perfect accuracy of 99.98%, with Precision, Recall, and F1-Score all reaching 99.98%. Most notably, the FPR was drastically reduced to 0.12%, ensuring a more reliable detection system with minimal false alarms.

Comparing the two scenarios, the SMOTE-RUS balanced approach significantly outperformed the imbalanced baseline by stabilizing the classification boundary and enhancing the model's sensitivity to attack patterns. The integration of feature visualization proved instrumental in refining feature selection, ensuring that the MobileNet architecture remained lightweight without compromising on robust detection capabilities. Ultimately, this approach provides a scalable and highly accurate solution for securing resource-constrained industrial environments against evolving cyber threats.

## 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. Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). In *Advances in computers* (Vol. 117, No. 1, pp. 129-164). Elsevier.

3. Abisoye, A., & Akerele, J. I. (2021). High-impact data-driven decision-making model for integrating cutting-edge cybersecurity strategies into public policy. *Governance, and Organizational Frameworks*.

4. Gade, K. R. (2021). Data-driven decision making in a complex world. *Journal of computational innovation*, *1*(1).

5. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.

6. Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*, *14*(2).

7. Taha, A. E. M., Rashwan, A. M., & Hassanein, H. S. (2020). Secure communications for resource-constrained IoT devices. *Sensors*, *20*(13), 3637.

8. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024). Data security of IoT devices with limited resources: challenges and potential solutions. *doors*, *3666*, 85-96.

9. Bian, J., Al Arafat, A., Xiong, H., Li, J., Li, L., Chen, H., . & Guo, Z. (2022). Machine learning in real-time Internet of Things (IoT) systems: A survey. *IEEE Internet of Things Journal*, *9*(11), 8364-8386.

10. Wu, X., Liu, C., Wang, L., & Bilal, M. (2023). Internet of things-enabled real-time health monitoring system using deep learning. *Neural Computing and Applications*, *35*(20), 14565-14576.

11. Alblooshi, H. (2024). *Optimizing Neural Networks for IIoT Attack Detection*. Rochester Institute of Technology.

12. Alli, A. A., Kalinaki, K., Fahadi, M., & Ibrahim, L. (2024). Securing industrial internet of things (iiot): A review of technologies, strategies, challenges, and future trends. *Artificial Intelligence Solutions for Cyber-Physical Systems*, 244-263.

13. Guo, Z., Tan, T., Liu, S., Liu, X., Lai, W., Yang, Y., . & Zhou, Y. (2023). Mitigating false positive static analysis warnings: Progress, challenges, and opportunities. *IEEE Transactions on Software Engineering*, *49*(12), 5154-5188.

14. Sivaraman, H. (2022). Adaptive Thresholding in ML-Driven Alerting Systems for Reducing False Positives in Production Environments. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *6*(10.55041).

15. Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., . & Hussain, A. (2024). Interpreting black-box models: a review on explainable artificial intelligence. *Cognitive Computation*, *16*(1), 45-74.

16. Nascita, A., Montieri, A., Aceto, G., Ciuonzo, D., Persico, V., & Pescapé, A. (2021). XAI meets mobile traffic classification: Understanding and improving multimodal deep learning architectures. *IEEE Transactions on Network and Service Management*, *18*(4), 4225-4246.

17. Alshamy, R., Ghurab, M., Othman, S., & Alshami, F. (2021, August). Intrusion detection model for imbalanced dataset using SMOTE and random forest algorithm. In *International Conference on Advances in Cyber Security* (pp. 361-378). Singapore: Springer Singapore.

18. Choudhary, V., Tanwar, S., & Choudhury, T. (2024). Evaluation of contemporary intrusion detection systems for internet of things environment. *Multimedia Tools and Applications*, *83*(3), 7541-7581.