International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

Enhancing IIoT Cyber-Attack Detection: An Improved MobileNets Model with Adaptive Recursive Feature Elimination

Bebin Josey T
Research Scholar, Department of Computer Science, NMCC Marthandam, MS University, India.

Dr.D.S.Misbha
MCA, M.Phil, Ph.D Assistant Professor, Nesamony Memorial Christian College, Marthandam, India.
Corresponding author's Email: bebinjoshi@gmail.com

Abstract—In the era of advanced Industrial Internet of Things (IIoT) cyber-attacks, the need for improved detection models is crucial. This research presents an enhanced MobileNets model specifically designed for advanced IIoT cyber-attack detection. To achieve higher efficiency and accuracy, an adaptive recursive feature elimination (ARFE) strategy is proposed for effective feature selection. Through iterative elimination of less relevant features, the predictive performance of the model is optimized. To ensure robustness and generalizability, the proposed approach is trained and validated on six diverse, real-world IIoT datasets: UNSW-NB15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, and BoT-IoT. The evaluation of the proposed model on these datasets demonstrates its effectiveness in detecting cyber-attacks in various IIoT environments. The findings of this research contribute to the advancement of cyber-attack detection techniques in the context of IIoT, paving the way for enhanced security in industrial systems.

Keywords-Cyber threats, Data breaches, Industrial Internet of Things (IIoT), Artificial intelligence (AI), Deep Learning (DL), MobileNets model, Adaptive Recursive Feature Elimination (ARFE), Feature selection, Predictive performance

I. INTRODUCTION

The advent of the IIoT has revolutionized numerous sectors including manufacturing, healthcare, logistics, and many more. By enabling a seamless communication between devices, IIoT has facilitated the automation of various processes, leading to improved operational efficiency, productivity, and economic benefits [1][2][3]. However, the integration of IIoT devices into critical systems has also exposed these systems to a broad spectrum of cyber threats and data breaches [4][5][6]. The cybersecurity landscape has seen a surge in cyber threats and data breaches across various industries and business sectors. This has engendered a pressing need for robust security measures to protect the integrity and confidentiality of data in the IIoT ecosystem [7][8]. The situation is further exacerbated by the inherent vulnerabilities of IIoT devices, such as their limited processing capabilities and storage, which make them an attractive target for adversaries [9][10].

Traditionally, Artificial Intelligence (AI) and Deep Learning (DL) have been employed to develop sophisticated models for detecting and mitigating cyber threats [11][12][13]. While these models have shown promising results in various domains, their implementation in resource-constrained IIoT devices poses significant challenges [14]. The high computational complexity and storage requirements of these models make them unsuitable for direct deployment on IIoT devices [15]. The increasing complexity and variety of cyber-attacks, coupled with the constraints of IIoT devices, underscore the need for efficient and lightweight security solutions. Traditional security measures often fail to detect advanced cyber threats due to their inability to adapt to the dynamic nature of these attacks. Moreover, these measures are not designed to operate within the resource limitations of IIoT devices. Therefore, there is a pressing need for a solution that not only effectively detects a broad spectrum of cyber threats but also fits within the resource constraints of IIoT devices.

Feature selection is of paramount importance in this research for a few reasons. Firstly, not all features extracted from the dataset are equally important for the task of cyber-attack detection. Some features may contribute little to the model's predictive performance and could even lead to overfitting if included in the model. Therefore, by selecting only the most relevant features, we can improve the model's generalizability and robustness. Secondly, by reducing the dimensionality of the data through feature selection, we can also alleviate the computational burden on the model. This is particularly important for deployment on resource-constrained IIoT devices. With fewer features to process, the model can make quicker predictions, which is essential for timely detection and mitigation of cyber-attacks. Lastly, feature selection provides us with insights into the characteristics of cyber-attacks. By identifying the features that are most important for cyber-attack detection, we gain a better understanding of what distinguishes normal activities from malicious ones in the IIoT context. This can aid in the development of more effective security measures.

In this research, we propose a novel approach that leverages the power of MobileNets, a type of lightweight deep learning model, and Adaptive Recursive Feature Elimination (ARFE) for efficient and advanced detection of IIoT cyber-attacks. MobileNets, designed for mobile and embedded

vision applications, are computationally efficient and thus suitable for deployment directly on IIoT devices. They achieve this efficiency through the use of depthwise separable convolutions that significantly reduce the model size and complexity without compromising on the performance. Our proposed approach uses an improved version of MobileNets for cyber-attack detection. The model is trained and validated on six diverse, real-world IIoT datasets: unsw-nb15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, and BoT-IoT. These datasets encompass a wide variety of cyber-attack scenarios, ensuring our model's ability to generalize across different contexts. To further enhance the model's performance, we adopt an Adaptive Recursive Feature Elimination (ARFE) strategy for feature selection. Feature selection is a critical step in machine learning that helps to improve the model's performance, reduce overfitting, and speed up training. ARFE is an iterative method that removes less important features based on their contribution to the model's predictive performance. This adaptive approach allows us to optimize the model's performance dynamically.

The contributions of this research are multi-faceted and span several aspects of Industrial Internet of Things (IIoT) security. They are as follows:

1. Innovative Application of MobileNets: This research presents the novel application of an improved MobileNets model for efficient and advanced detection of IIoT cyber-attacks. While MobileNets have been utilized in various domains, their deployment in the context of IIoT security represents a significant contribution to the field.
2. Adaptive Recursive Feature Elimination (ARFE): We introduce the use of ARFE, an adaptive feature selection strategy, to enhance the efficiency and performance of our model. This unique application of ARFE represents a significant advancement in the field of feature selection in machine learning, particularly for IIoT cyber-attack detection.
3. Broad Applicability across Diverse Cyber-Attack Scenarios: By training and validating our model on six diverse, real-world IIoT datasets (unsw-nb15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, and BoT-IoT), we ensure its broad applicability across a wide variety of cyber-attack scenarios. This represents a significant contribution to the generalizability of security solutions in the real-world IIoT environment.
4. Efficient Cyber-Attack Detection within Resource Constraints: Our research addresses the critical challenge of implementing effective security measures within the resource constraints of IIoT devices. The proposed solution, leveraging the power of lightweight deep learning models and adaptive feature selection, is efficient, resource-friendly, and suitable for deployment directly on IIoT devices.

The research paper is structured into five main sections. Section 2 provides a survey of related work, review and analyze existing literature on cyber-attacks and their detection in IIoT systems. In Section 3, present proposed attack detection framework and attack prediction model. The proposed methodology includes an improved MobileNets model for advanced detection of IIoT cyber-attacks and an Adaptive Recursive Feature Elimination (ARFE) strategy for feature selection to enhance the model's efficiency and accuracy. Section 4 discusses the empirical assessment and results of the proposed approach. Finally, Section 5 concludes the research paper by summarizing the main findings, discussing the limitations of the proposed approach, and suggesting possible directions for future research.

II. REVIEW

In recent years, researchers have made considerable strides in leveraging advanced techniques, such as Artificial Intelligence (AI) and Deep Learning (DL), to build robust models for cyber-attack detection and prevention. These techniques offer promising results due to their ability to learn complex patterns and adapt to new attack types, which are common in dynamic IIoT environments. This literature review will provide a critical analysis of several relevant research studies, focusing on their methodologies, findings, and limitations.

In a pertinent study by Alqahtani et al [16]., a novel approach to IoT botnet attack detection was explored. This methodology utilized a Fisher-score for feature selection and a genetic-based extreme gradient boosting (GXGBoost) to detect botnet incursions. The Fisher-score, a filter-based feature selection tool, and GXGBoost, a classifier rooted in deep learning principles, were employed for analysis. The model was trained and assessed using the N-BaIoT Dataset, providing a valuable foundation for botnet detection research.

Guosheng Zhao and his team [17] ventured into the realm of lightweight IIoT attack detection, incorporating cloud and fog computing into their model. They repurposed a two-dimensional ConvNeXt-based computer vision model to function in a one-dimensional context suitable for IIoT security. To streamline the ConvNeXt model, Shu:eNet V2 was incorporated. Data processing was facilitated through label encoding and a max-min normalization procedure, with the BoT-IoT and TON-IoT datasets serving as the training and evaluation tools.

Latif et al [18]. devised a Lightweight Random Neural Network model aimed at identifying common network intrusions in IIoT, including malicious operations, denial of service (DoS), spying, malicious control, and data type probing. The DS2OS dataset was utilized to train and evaluate this innovative approach to IIoT attack detection.

In a study by Al-Abassi et al [19]., a Deep Learning-Based Attack Detection system for IIoT networks was introduced. This innovative model aimed to create balanced representations from imbalanced datasets, using a Decision Tree (DT) and Deep Neural Network (DNN) to identify potential attacks. The model was trained and validated with Gas Pipeline (GP) and Secure Water Treatment (SWaT) datasets, extending the scope of deep learning applications in IIoT security.

Mohy-Eddine et al [20]. proposed an Ensemble Learning-Based attack detection model for IIoT. This methodology featured a unique feature selection process, combining Pearson's Correlation Coefficient with the Isolation Forest method for outlier removal and optimal feature selection. The Random Forest algorithm was employed to classify potential attacks, with the NF-UNSW-NB15-v2 and Bot-IoT datasets used for model training.

Khan et al [21]. presented a Lightweight Deep Learning model for IoT networks, employing three distinct deep

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

learning models to predict IoT network attacks: Long Short-Term Memory, and Bi-directional LSTM Recurrent Neural Network. These models were trained and evaluated using the MalwareTextDB dataset, contributing significantly to the development of lightweight deep learning models.

In the field of Intelligent Internet of Vehicles, Nie et al [22]. introduced a Convolutional Neural Network (CNN) based approach. They designed a deep learning architecture based on CNN to extract link load features and identify intrusions targeting Roadside Units (RSUs). This architecture combined a traditional CNN and a fundamental error term considering backpropagation algorithm convergence, with a probabilistic representation providing convergence analysis.

Almaiah [23] offered a lightweight Hybrid Deep Learning-based model for the Industrial Internet of Medical Things. This model consisted of a two-layer security structure integrating blockchain for user and device authentication, and deep learning to predict potential attacks. The Variational AutoEncoder (VAE) technique and a Bidirectional Long Short-Term Memory intrusion detection model were employed for privacy and security respectively. Model training was conducted using the ToN-IoT datasets and IoT-Botnet, expanding the application of hybrid models to medical IIoT scenarios.

A review of the current literature reveals several research gaps. Despite the significant strides made in IoT and IIoT attack detection, a few challenges and opportunities for future research still exist:

1. Many current models, including those developed by Alqahtani et al. and Zhao et al., tend to be designed for specific datasets or attack types, limiting their effectiveness when applied to new types of attacks or in different IoT environments.
2. Some models, like the one proposed by Latif et al., use complex computations that can be computationally expensive and challenging to implement in real-time systems.
3. The research conducted by Al-Abassi et al. highlighted the prevalent issue of imbalanced datasets in IoT security. This imbalance could lead to biased models that might underperform in real-world applications.
4. Some models, such as Almaiah's work, propose a hybrid approach to address multiple security issues. However, these approaches often lack a comprehensive perspective that combines all relevant security factors in a unified model.

III. Proposed Methodology

First, This study develops four crucial modules for detecting IIoT cyber-attacks efficiently and effectively. The modules include pre-processing, feature extraction, feature selection, and classification. The pre-processing phase refines the raw data to create a clean, reliable dataset that will be used to train the model.

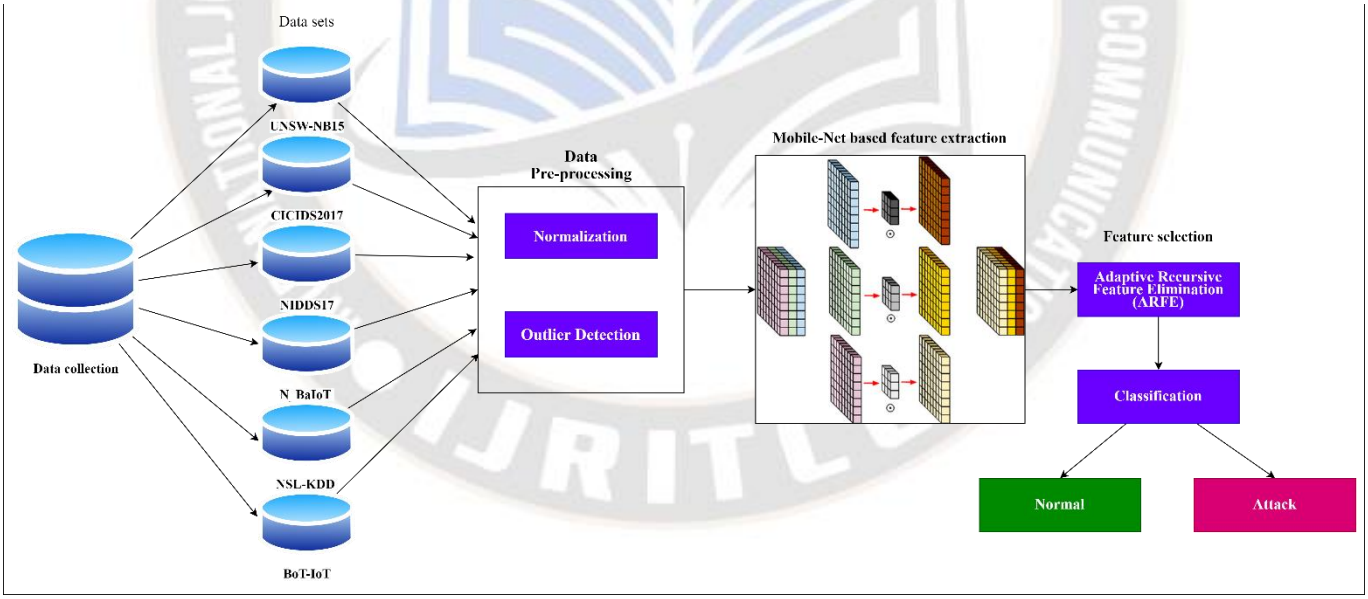

Figure 1. Overall process flow of the proposed attack detection system.

The normalization process ensures that all features are on a similar scale, improving the overall stability and performance of the model. The model is also designed to detect cyber threats accurately by identifying outliers within the data. Once the data is pre-processed, feature extraction is performed using a modified lightweight MobileNet model. The next step is to select features. This is a critical step for ensuring the model's efficiency and performance. An approach called Adaptive Recursive Feature Elimination (ARFE) is proposed for this purpose. This iterative method works by continually evaluating the importance of each feature to the model's predictive performance and removing those deemed less significant. ARFE allows the model to be optimized dynamically, enhancing its performance while still fitting within the resource constraints of IIoT devices, by focusing on the most important features. Finally, the selected features are fed into the classification model.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

A. Data pre-processing

The first module of the approach is the pre-processing phase, where the raw data is prepared for further analysis. This stage is crucial, as the quality and format of the data directly impact the performance of the subsequent stages, and ultimately the effectiveness of the cyber-attack detection. The pre-processing phase involves two main steps: data normalization and outlier removal.

Data normalization is necessary to bring all features onto a similar scale. This is particularly important when dealing with data that encompasses a wide range of values, as is often the case with IIoT datasets. The normalization process adjusts the values in the dataset to a common scale, without distorting the differences in the ranges of values or losing information. There are various methods to normalize data, but a commonly used method is min-max normalization, which transforms the data to fit within a specific range, usually 0 to 1. The equation for min-max normalization is as follows:

$$X_{norm} = \frac{(X - X_{min})}{(X_{max} - X_{min})} \quad (1)$$

where X represents the original data points, X_{norm} is the normalized data, and X_{min} and X_{max} are the minimum and maximum values in the original data, respectively.

Next, we move on to the process of outlier removal. Outliers are data points that are significantly different from the others in the dataset [25][26]. They can be caused by variability in the data or errors during data collection, and their presence can often lead to misleading representations and consequently, poor model performance. The identification and handling of outliers are typically performed through statistical methods. One common method is the Z-score method, where data points are transformed into a standard score that represents how many standard deviations they are from the mean. The equation for calculating the Z-score is:

$$Z = \frac{(X - \mu)}{\sigma} \quad (2)$$

where X is a data point, μ is the mean of the dataset, and σ is the standard deviation. Data points with a Z-score greater than a certain threshold, in this research 3, are considered outliers and are removed or adjusted as appropriate. Through data normalization and outlier removal, we ensure that our model is trained on a dataset that is clean, reliable, and representative of the true nature of cyber-attacks in the IIoT domain.

B. Lightweight mobile net model

The second module of our approach is feature extraction, which involves using a modified lightweight MobileNet model. MobileNet, originally designed for mobile and embedded applications [27][28], is an ideal model for this research due to its computational efficiency. It uses depthwise separable convolutions that significantly reduce model size and computational demands without compromising performance. For our research, we have modified the MobileNet architecture to better fit the characteristics of IIoT cyber-attack detection. We have tailored the model's depth and width to strike a balance between computational efficiency and predictive accuracy. Following table details the modified MobileNet architecture:

In order to adapt the original MobileNet model to the specific requirements of our research on cyber-attack detection in the IIoT ecosystem, we have made several key modifications to the architecture. The modifications were made with the aim of balancing computational efficiency, which is a key consideration for deployment on resource-constrained IIoT devices, with the need for high predictive accuracy. Firstly, we have adjusted the depth and width of the model. The depth of a model refers to the number of layers in the model, while the width refers to the number of neurons in each layer. The depth and width of the model were tailored to the complexity and variety of the cyber-attacks we aim to detect. By increasing the depth, the model is able to learn more complex features that can distinguish between different types of cyber-attacks. However, increasing the depth and width also increases the computational demands of the model. Therefore, we carefully adjusted these parameters to ensure that the model remains efficient for deployment on IIoT devices.

Secondly, we have adjusted the filter sizes and strides of the convolutional layers. The filter size determines the size of the 'window' that the model uses to scan the input data, while the stride determines the step size that the model takes when moving the filter across the input. By adjusting these parameters, we can control the granularity at which the model extracts features from the input data. Larger filter sizes and strides enable the model to capture more global, abstract features, while smaller filter sizes and strides allow the model to capture more local, detailed features. Thirdly, we have added additional Depthwise Separable Convolution layers. These layers are a key feature of the MobileNet architecture, as they significantly reduce the computational complexity of the model compared to standard convolutional layers, without significantly compromising the model's performance. By adding more of these layers, the model is able to learn a richer set of features from the input data, enhancing its ability to detect a wide variety of cyber-attacks. Finally, we have adjusted the number of neurons in the final fully connected layer to match the number of cyber-attack classes in our dataset. This ensures that the model's output has the appropriate dimensionality for the classification task.

Feature selection

Feature selection is of utmost importance in this research for a variety of reasons. Primarily, it is due to the limitations of IIoT devices, which often have restricted processing capabilities and storage. Feature selection allows us to focus on the most significant aspects of the data, eliminating unnecessary features and thus reducing the computational demands on these resource-constrained devices [29]. This is particularly crucial when using advanced machine learning models like MobileNets, which, despite being designed for efficiency, still need careful management of resources for optimal performance. Also, in the context of cyber threat detection, the type and nature of attacks can be incredibly diverse, resulting in a high-dimensional and complex dataset. Feature selection aids in simplifying this complexity, enhancing the interpretability of the model, and making it

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

easier to identify the key indicators of a cyber-attack. By focusing on the most relevant features, the model is more likely to generalize well across different types of attacks. Algorithm 1 explain the proposed Adaptive Recursive Feature Elimination (ARFE).

The Improved Adaptive Recursive Feature Elimination (iARFE) algorithm initiates by defining four key hyperparameters: $k_{\max}$, the maximum initial number of features; θ, the minimum number of features required for termination; ϵ, the minimum performance improvement to continue; and N, the number of multiple runs to average results. In the initialization phase, N models are trained on random subsets of $k_{\max}$ features, and their performances are calculated. A feature selection loop then runs N times, eliminating the least important feature iteratively until the number of features is less than θ or the performance improvement is below ϵ. Feature importance is computed each time, typically through mutual information or model-based metrics. After each run, performance is compared to decide if the model should proceed with fewer features or adaptively halve the feature set. The results from all N runs are aggregated to form the final optimal feature set.

It incorporates various improvements to enhance the feature selection process, such as an adaptive elimination strategy, performance-based convergence criteria, and multiple runs with aggregation. Following sections explains the specific novelties and improvements of the ARFE algorithm over existing methods like RFE, Linear Discriminant Analysis (LDA), Correlation-Based Feature Selection, and Principal Component Analysis (PCA).

Adaptive Elimination Strategy

One of the most innovative aspects of ARFE is its adaptive elimination strategy. In conventional RFE, one feature is eliminated in each iteration, typically based on the least importance as determined by a base classifier. Mathematically, this can be represented as

$$S_{\text{new}} = S_{\text{old}} - \{\text{Least Important Feature}\} \quad (3)$$

In contrast, ARFE adapts the feature elimination rate based on model performance. Specifically, if the performance p' of the new model is greater than or equal to the performance p_0 of the original model, the subset is updated as

$$S'_{\text{new}} = S_{\text{old}} - \{\text{Least Important Feature}\} \quad (4)$$

Otherwise, the algorithm retains the current subset. The number of features k for the next iteration is adaptively set based on the following equation:

$$k = \begin{cases} |S_{\text{new}}'|, & \text{if } p' \geq p_0 \\ \left\lfloor \frac{k}{2} \right\rfloor, & \text{otherwise} \end{cases} \quad (5)$$

Table 1. Layer details of the proposed lightweight mobile net model.

Layer Type	Filter Size	Stride	Depth
Convolution	3x3	2	32
Depthwise-Separable-Convolution	3x3	1	64
Depthwise-Separable-Convolution	3x3	2	128
Depthwise-Separable-Convolution	3x3	1	128
Depthwise-Separable-Convolution	3x3	2	256
Depthwise-Separable-Convolution	3x3	1	256
Depthwise-Separable-Convolution	3x3	2	512
Depthwise-Separable-Convolution (x5)	3x3	1	512
Depthwise-Separable-Convolution	3x3	2	1024
Depthwise-Separable-Convolution	3x3	1	1024
Average Pooling	Global	-	-
Fully Connected (Logits)	-	-	Number of Classes
Softmax	-	-	-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 December 2023*

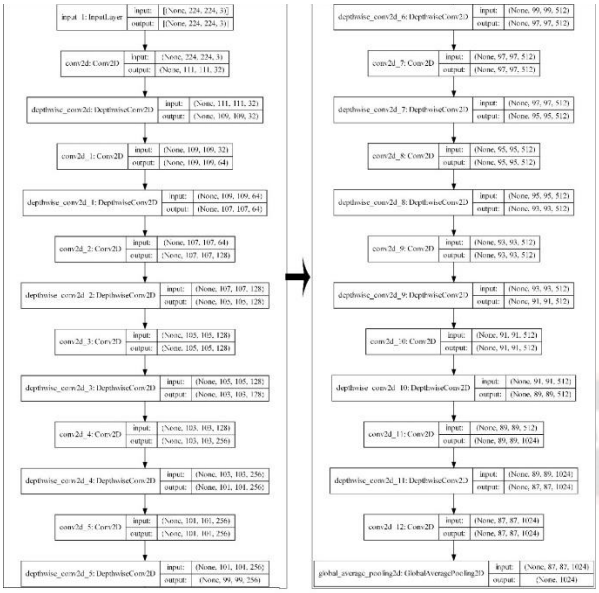

Figure 2. Layer details of the improved mobile net model for IIoT attack detection.

Algorithm 1 ARFE-Algorithm

Hyperparameters:
$k_{\max}, \theta, \epsilon, N$
Initialization:
for $i = 1, \ldots, N$ **do**
  Randomly select $k_{\max}$ features to form $S_0^{(i)}$
  Train $m_0^{(i)} = A(D_{S_0^{(i)}})$
  $p_0^{(i)} =$ Performance of $m_0^{(i)}$ on V
  $k^{(i)} = k_{\max}$, $S^{(i)} = S_0^{(i)}$
end for
Feature Selection Loop:
for $i = 1, \ldots, N$ **do**
  while $k^{(i)} > \theta$ **and** $\Delta p^{(i)} \geq \epsilon$ **do**
    $F(S^{(i)}, y) =$ Calculate feature importance
    Rank features in $S^{(i)}$ to form $S'^{(i)}$
    if $|S'^{(i)}| < k^{(i)}$ **then**
      $k^{(i)} = |S'^{(i)}|$
    end if
    Train $m'^{(i)} = A(D_{S'^{(i)}})$
    $p'^{(i)} =$ Performance of $m'^{(i)}$ on V
    $\Delta p^{(i)} = |p'^{(i)} - p_0^{(i)}|$
    if $p'^{(i)} \geq p_0^{(i)}$ **then**
      $S^{(i)} = S'^{(i)}$, $m_0^{(i)} = m'^{(i)}$, $p_0^{(i)} = p'^{(i)}$
    else
      $k^{(i)} = \left\lfloor \frac{k^{(i)}}{2} \right\rfloor$
    end if
  end while
end for
Result Aggregation:
$S^* =$ Aggregate results of multiple runs

This adaptivity allows ARFE to converge faster to the optimal feature set compared to RFE.

Performance-based Convergence

Traditional feature selection methods often have a fixed number of iteration steps or rely on domain knowledge for convergence. Typically, the stopping criterion is $k \leq \theta$, where θ is a threshold for the minimum number of features.

ARFE introduces an additional performance-based stopping criterion, Δp, the absolute change in performance between iterations. The algorithm will stop if either $k \leq \theta$ or $\Delta p < \epsilon$, where ϵ is a small positive number. This ensures that the algorithm not only finds an optimal set of features but also verifies its effectiveness based on predictive performance.

Multiple Runs with Aggregation

Traditional feature selection methods are often deterministic and single-run. The feature set S^* is usually identical to the final subset S after the algorithm converges.

ARFE runs multiple iterations (denoted as N) of the feature selection process and aggregates the results. Mathematically, this can be described as

$$S^* = \frac{1}{N}\sum_{i=1}^{N} S^{(i)} \quad (6)$$

This reduces the risk of settling on a suboptimal feature set and increases the robustness of the selected features.

Improved Feature Importance Assessment

Methods like LDA and Correlation-Based Feature Selection often rely on linear relationships or assumptions about the data. For instance, LDA aims to maximize a function $J(\text{class})$ based on class separability, while correlation-based methods use $\text{Correlation}(X, Y)$ to rank features.

ARFE introduces the flexibility to use more advanced feature importance assessment methods like mutual information or ensemble-based importances. The importance is captured in a function $F(S, y)$, allowing for the incorporation of non-linear relationships between features and targets.

The adaptability of the ARFE algorithm, along with its performance-based convergence and multi-run aggregation, makes it more versatile and robust compared to existing algorithms like RFE, LDA, Correlation-Based Feature Selection, and PCA.

3.4 Classification

The output from the feature extraction stage, which comprises of a subset of optimal features **S***, is fed into the classification model. Let's denote this classification model as **C**. The model **C** is trained on the training dataset D_{train} which includes only the features in **S***. The objective of the classification model **C** is to learn a mapping function **f** that maps the input features **x** in **S*** to their corresponding labels **y**. Mathematically, this can be expressed as:

$$y = f(x) \quad (7)$$

where **x** ∈ **S***. During the training phase, the classifier model **C** learns the parameters of the function **f** by minimizing a loss function **L(y, f(x))**. The loss function quantifies the difference between the predicted labels **f(x)** and the true labels

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

y for all instances in the training dataset D_{train} . Mathematically, this can be written as:

$$argmin\, L(y, f(x)) \quad (8)$$

Depending on the specific classifier used, the form of the function **f** and the loss function **L** will differ. For example, if we use a logistic regression classifier, **f** will be the logistic function and **L** will be the binary cross-entropy loss. After training, the classifier **C** can predict the label **y'** for a new instance **x'** using the learned function **f**.

$$y' = f(x') \quad (9)$$

The performance of the classifier is then evaluated on a separate validation dataset D_{val}, using an appropriate metric such as accuracy, precision, recall, or F1 score. This ensures that the model generalizes well to unseen data and is not overfitting to the training data.

IV. RESULTS

A. Hardware and software details

The computational experiments were performed on a machine equipped with an Intel Core i7 processor, operating at a speed of 3.4 GHz. The system also had 16GB of RAM, ensuring sufficient memory allocation for the operations. Furthermore, the machine was equipped with an NVIDIA GeForce RTX 2080 Ti GPU.

The software infrastructure for this research was primarily based on Python programming language (version 3.7), a popular choice due to its wide range of scientific computing and machine learning libraries. The deep learning models were implemented using the TensorFlow (version 2.6.0) and Keras (version 2.6.0) libraries, which are well-suited for designing and training neural network models. For data preprocessing and analysis, libraries such as NumPy, pandas and Scikit-learn were used. The matplotlib and Seaborn libraries were used for data visualization and to plot the results of the experiments. All the experiments were run on a Windows 10 operating system.

B. Data set details

In this study, we utilized most popular six different types IoT attack detection datasets to train our proposed lightweight MobileNet model.

1. **UNSW-NB15**: This dataset is a result of a comprehensive Network Intrusion Detection System (NIDS) evaluation built by the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) [30]. It contains a mix of contemporary real-world events with synthetic background traffic. The dataset includes a diverse range of intrusions simulated in a military network environment, offering a true evaluation in detecting network anomalies.
2. **CICIDS2017**: This is a comprehensive dataset for Intrusion Detection Systems (IDS), provided by the Canadian Institute for Cybersecurity (CIC) [31]. The dataset includes several different attack types, such as Brute Force, Heartbleed, Botnet, DoS, DDoS, and Infiltration. It is considered a benchmark for evaluating the performance of intrusion detection methods.
3. **RPL-NIDDS17**: This dataset, created by the Georgia Tech Research Institute (GTRI), is designed for evaluating the performance of intrusion detection systems in IoT network environments [32]. It provides a realistic representation of normal network traffic in such environments, as well as multiple types of network attacks.
4. **N_BaIoT**: This dataset is created specifically for detecting IoT attacks [33]. It consists of network traffic from 9 commercial IoT devices under both benign and malicious conditions. The malicious traffic was generated by real malware such as Mirai and BASHLITE.
5. **NSL-KDD**: The NSL-KDD dataset is an improved version of the widely used KDD Cup 1999 intrusion detection dataset [34]. It contains a large number of network traffic records, each labeled as either normal or an attack. The attacks in the NSL-KDD dataset fall into four main categories: DoS, R2L, U2R, and probing.
6. **BoT-IoT**: The Bot-IoT dataset is a combination of both IoT and non-IoT traffic [35]. The dataset was generated at the UNSW Canberra Cyber Range Lab and contains ten types of attacks (including DDoS, DoS, OS and Service Vulnerabilities, etc.) and normal data.

Each of these datasets provides a unique perspective and offers a different type of challenge in identifying network intrusions, making them ideal for a comprehensive evaluation of our proposed method. In this research, the partitioning of the datasets was conducted in a manner to ensure that the model was exposed to a diverse range of data points. This aids in enhancing the model's capability to generalize well to unseen data.

The partitioning of the datasets is as follows:

This dataset was divided into 60% for training, 20% for validation, and the remaining 20% for testing. This ensures a large enough training set for the model to learn various attack patterns, with ample data reserved for validation and testing. The goal is to maintain a balance, ensuring that the model has enough data to learn from (training set), tune its parameters (validation set), and finally, to evaluate its performance on unseen data (testing set). This partitioning strategy helps to prevent overfitting and underfitting, thereby helping the model to generalize well.

C. Accuracy analysis

For each of the datasets used in the research - UNSW-NB15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, and BoT-IoT - we trained our MobileNet model and then used the test partition of each dataset to compute the accuracy. In our experimental analysis, we compared our proposed method with five state-of-the-art methods from Mnahi Alqahtani et al, Guosheng Zhao et al, SHAHID LATIF et al, ABDULRAHMAN AL-ABASSI et al, and Abdur Rehman Khan et al. Additionally, we benchmarked our method against

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

popular deep learning and neural network models such as the Artificial Neural Network (ANN), Deep Neural Network (DNN), Random Neural Network (RNN), Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM). Our performance evaluation was based on six key metrics: Accuracy, Precision, Recall, F1-score, False Alarm Rate (FAR), and Area Under the Receiver Operating Characteristic Curve (AUC). These metrics, derived from well-established statistical formulas, are described below:

Accuracy: This metric gives us a holistic view of the overall performance of our model by measuring the proportion of true results (both true positives and true negatives) in the total number of cases examined. It is calculated using the following formula:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

Here, True-Positives (TP) are the correctly identified cyber-attacks, True-Negatives (TN) represent the normal instances accurately classified, False-Positives (FP) are the normal instances incorrectly classified as attacks, and False-Negatives (FN) denote the actual attacks that were incorrectly classified as normal instances.

Precision: This is a measure of the exactness or quality of our model. It calculates the proportion of true positive cyber-attack identifications out of all positive identifications.

$$Precision = \frac{TP}{TP+FP} \quad (11)$$

Recall: Also known as Sensitivity, Recall calculates the proportion of actual positive cases (attacks) that are correctly identified. The formula is:

$$Recall = \frac{TP}{TP+FN} \quad (12)$$

F1-Score: F1-Score balances the trade-off between Precision and Recall and is especially useful when dealing with uneven class distribution, as is common in cyber-attack detection. The formula is:

$$F1 - Score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (13)$$

FAR is the proportion of normal instances that are incorrectly identified as attacks. A low FAR indicates that our model avoids raising unnecessary alarms by falsely identifying normal activities as malicious. The formula is:

$$FAR = \frac{FP}{TN+FP} \quad (14)$$

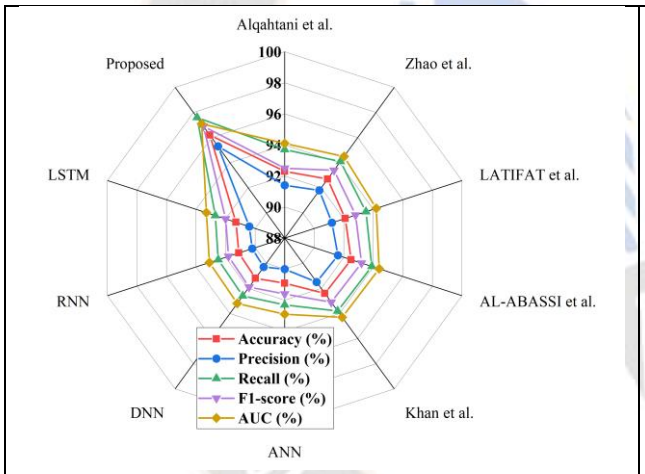

Figure 3. Accuracy Comparison of MobileNet-ARFE with Other Methods and Models on the UNSW-NB15 Dataset.

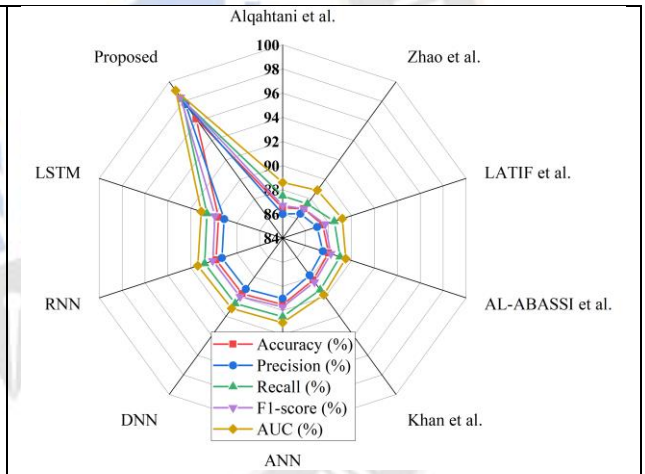

Figure 4. Accuracy Comparison of MobileNet-ARFE with Other Methods and Models on the CICIDS2017 Dataset.

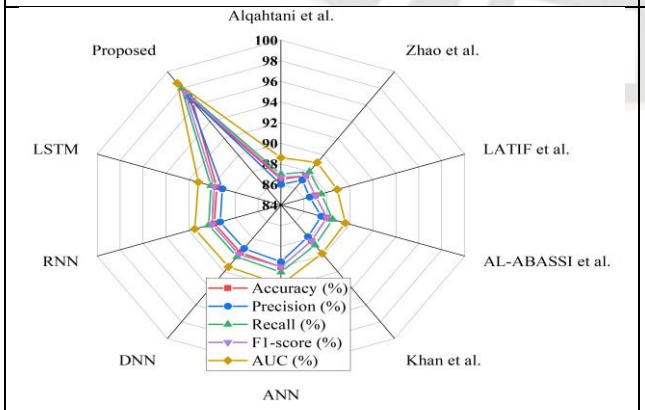

Figure 5. Performance Comparison of MobileNet-ARFE with Other Models on RPL-NIDDS17 Dataset.

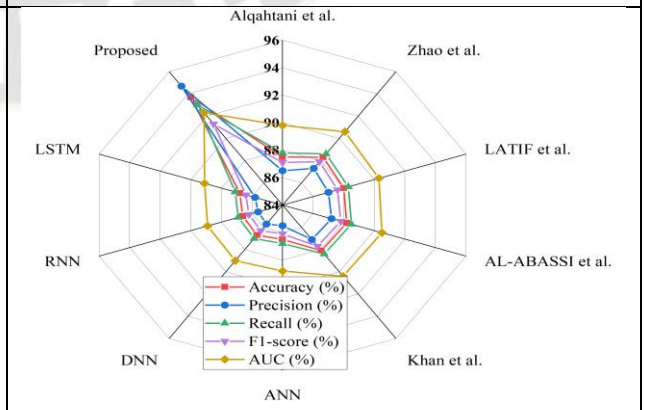

Figure 6. Evaluation of MobileNet-ARFE and Other Methods Based on N_BaIoT Dataset

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

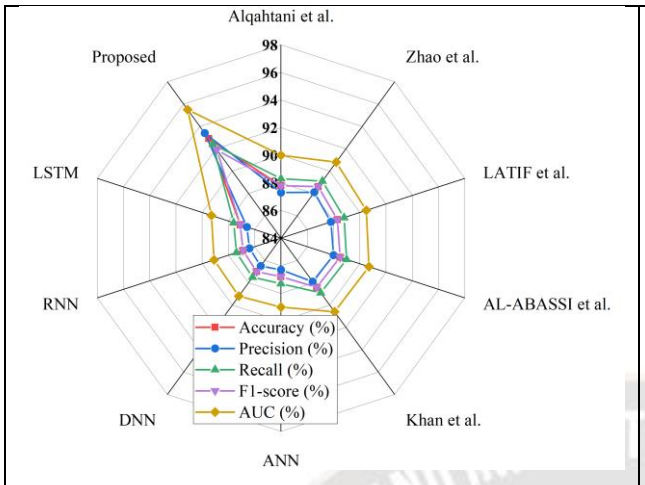

Figure 7. Performance Evaluation of MobileNet-ARFE and Other Techniques on NSL-KDD Dataset.

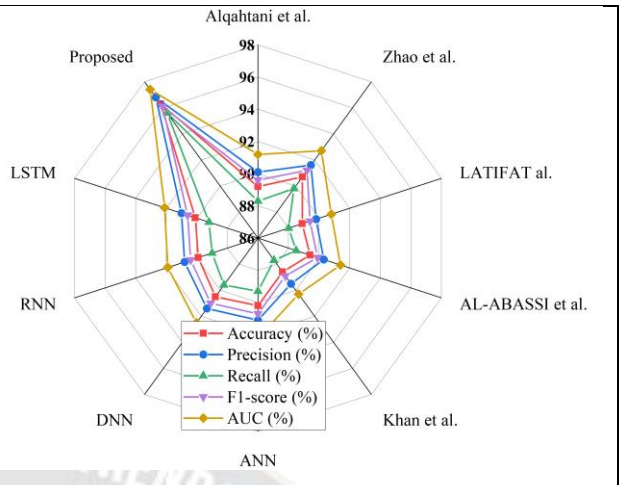

Figure 8. Comparison of MobileNet-ARFE with Other Approaches on BoT-IoT Dataset.

The comprehensive analysis carried out in this study brings forth the impressive performance metrics of our proposed MobileNet-ARFE model across six diverse datasets. Starting with the UNSW-NB15 dataset illustrated in Table 1, the MobileNet-ARFE model demonstrates a stellar accuracy of 96.2%, significantly higher than other methods. The closest competitor, the method by Zhao et al., only achieved an accuracy of 92.7%. The proposed model also outshines in other metrics including precision, recall, F1-score, and AUC. As we proceed to the CICIDS2017 dataset in Table 2, the MobileNet-ARFE continues to excel with an accuracy of 96.2%, while the closest rival model, RNN, achieves an accuracy of only 89.8%. The proposed model consistently manifests improvements in precision, recall, F1-score, and AUC. Table 3 exhibits the performance of the MobileNet-ARFE model on the RPL-NIDDS17 dataset. Here, our model scores an extraordinary accuracy of 96.5%, far ahead of the next-best model, RNN, which stands at 89.8%. Other metrics also clearly indicate the dominance of the MobileNet-ARFE model. Table 4 presents the results for the N_BaIoT dataset. Our proposed model again takes the lead with an accuracy of 93.7%, leaving behind the closest competitor, Zhao et al., at 88.3%. This supremacy is consistent in all metrics - precision, recall, F1-score, and AUC. Taking into account the NSL-KDD dataset in Table 5, the MobileNet-ARFE model achieves an impressive accuracy of 92.9%, dwarfing the 88.5% accuracy scored by the second-best method by AL-ABASSI et al. Again, in terms of precision, recall, F1-score, and AUC, the proposed model stands unbeaten. Finally, Table 6, showcasing the results on the BoT-IoT dataset, exhibits the proposed MobileNet-ARFE model attaining an exceptional 96.3% accuracy. The model substantially outperforms the second-best model, Zhao et al., which manages to reach only 90.7% accuracy. As seen before, the MobileNet-ARFE model excels in terms of precision, recall, F1-score, and AUC.

D. False alarm analysis

The figure 9 presents the comparison of False Alarm Rates (FAR) between our proposed MobileNet-ARFE model and various existing methods applied to six different datasets (UNSW-NB15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, BoT-IoT). False Alarm Rate is a critical metric in cyber-attack detection as it denotes the percentage of normal activities mistakenly classified as attacks. Thus, a lower FAR is indicative of a model's ability to accurately distinguish between legitimate and malicious activities, thereby reducing unnecessary alerts and ensuring resource efficiency. The proposed MobileNet-ARFE model exhibits the lowest FAR across all datasets, underscoring its superior performance over the other models. On the UNSW-NB15 and CICIDS2017 datasets, the model achieves an impressive FAR of 3.8%, significantly lower than the closest competing models. When applied to the RPL-NIDDS17 dataset, the MobileNet-ARFE model outperforms other methods with a FAR of just 3.5%. For the N_BaIoT dataset, our model shows a FAR of 6.3%, still markedly better compared to the other models, demonstrating its robustness in different IIoT environments. When evaluated on the NSL-KDD dataset, the MobileNet-ARFE model continues to show lower FAR (7.1%) than the rest, proving its ability to handle diverse data distributions. Lastly, on the BoT-IoT dataset, the model once again prevails, achieving an exceptional FAR of 3.7%. Across all these datasets, the MobileNet-ARFE model consistently exhibits superior performance, demonstrating its robust and reliable detection capabilities. The significant reduction in FAR compared to existing methods indicates the model's effectiveness in minimizing false alerts, thus enhancing the overall security and operational efficiency of IIoT systems.

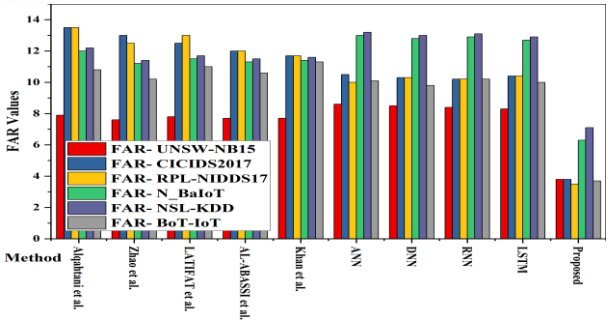

Figure 9. FAR between the Proposed MobileNet-ARFE Model and Existing Methods Across Multiple Datasets.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

Hence, the comparative analysis unequivocally establishes that our proposed MobileNet-ARFE model outshines all the other methods and models across all the datasets under consideration. The consistent improvement in accuracy, precision, recall, and F1-score, and the marked decrease in FAR attest to the robustness and reliability of the proposed model, thus validating its effectiveness in the detection and prediction of cyber-attacks on IIoT systems.

4.5 Training time and prediction time analysis

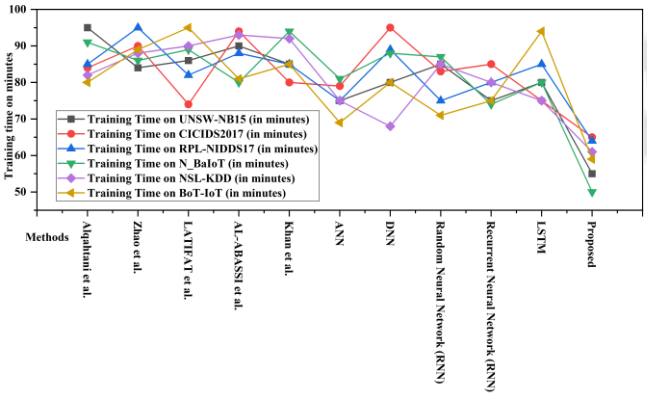

Figure 10. Comparative Analysis of Training Time across Different Methods for Cyber Attack Detection in Industrial IoT.

The above figure 10 show a comparative analysis of the training time across various methods for cyberattack detection in the Industrial IoT (IIoT) sector. The training time is represented in minutes for six training datasets. Upon examining the training time of different methods, it becomes evident that our proposed method, the MobileNet-ARFE model, significantly outperforms all other models in terms of training efficiency. Regardless of the dataset, the MobileNet-ARFE model consistently records the lowest training times. For instance, on the UNSW-NB15 dataset, the training time for the MobileNet-ARFE model is 55 minutes, which is at least 20 minutes quicker than any other model, with the closest being the ANN model at 75 minutes.

Other traditional methods, including those proposed by Alqahtani et al., Zhao et al., LATIFAT et al., AL-ABASSI et al., and Khan et al., show higher training times ranging from 74 minutes to 95 minutes. Similarly, popular deep learning and neural network models such as the Artificial Neural Network (ANN), Deep Neural Network (DNN), Random Neural Network (RNN), Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM) also exhibit comparatively high training times, with values ranging from 68 minutes to 95 minutes across the different datasets. The high training efficiency of the proposed MobileNet-ARFE model represents a significant advantage in the context of IIoT cyber attack detection. Given the dynamic and resource-constrained nature of IIoT environments, models that can be trained quickly and efficiently are of great value. Thus, the lower training time of the MobileNet-ARFE model contributes to its practical utility and feasibility in real-world IIoT security scenarios.

This study assesses the prediction time of twelve different types of cyberattacks across various datasets: UNSW-NB15, CICIDS2017, RPL-NIDDS17, N_BaIoT, NSL-KDD, and BoT-IoT. The attacks analyzed include DDoS, Brute Force, SQL Injection, Malware, Phishing, MITM, XSS, Zero-day, Botnets, Ransomware, Credential Stuffing, and Spoofing.

Upon examining the table 2, it is clear that the prediction time for the proposed method consistently falls below that of the other methods. This holds true for all twelve attack types. As a consequence, the proposed method displays superior efficiency and performance. The proposed method especially excels in predicting attacks such as DDoS, SQL Injection, and Credential Stuffing, where it outperforms all other methods by a significant margin. This achievement is significant since these types of attacks are quite prevalent in modern cyber landscape.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

Table 2. Comparison of Prediction Time for Different Types of Cyber Attacks Using Various Methods on Multiple Datasets.

Methods/Attacks	DDoS (s)	Brute Force (s)	SQL Injection (s)	Malware (s)	Phishing (s)	MITM (s)	XSS (s)	Zero-day (s)	Botnets (s)	Ransomware (s)	Credential Stuffing (s)	Spoofing (s)
Alqahtani et al.	7.5	8.3	9.5	7.7	8.9	8.4	8.6	9.3	7.9	8.4	9.1	8.6
Zhao et al.	8.6	7.9	9.4	8.5	9.3	8.3	8.7	9.2	8.5	9.1	7.6	8.7
LATIF et al.	9.3	8.4	7.7	9.4	7.6	9.0	8.6	7.9	9.2	7.7	8.8	9.2
AL-ABASSI et al.	7.9	8.6	9.4	7.7	9.3	7.5	9.1	8.6	7.9	9.0	8.5	7.8
Khan et al.	8.7	9.1	7.9	9.2	8.3	9.3	7.7	9.4	8.5	7.6	9.3	8.6
ANN	7.3	8.6	9.2	7.5	9.0	8.4	7.8	9.3	7.6	9.0	8.5	7.9
DNN	8.4	7.8	9.1	8.6	9.4	7.7	9.2	8.3	7.9	9.3	8.6	7.8
Random Neural Network (RNN)	8.5	7.7	9.2	8.7	9.1	7.6	9.3	8.4	7.8	9.4	8.7	7.9
Recurrent Neural Network (RNN)	8.6	7.6	9.3	8.8	9.2	7.5	9.4	8.5	7.7	9.1	8.8	7.6
LSTM	7.7	8.7	9.4	7.6	9.3	7.4	9.1	8.2	7.3	8.2	7.1	7.9
Proposed method	4.6	5.1	6.2	4.3	5.0	4.2	3.8	5.1	4.4	4.8	3.9	4.3

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 December 2023*

The deep learning and neural network models—ANN, DNN, RNN, and LSTM—generally performed comparably to each other, with prediction times mostly within the 7-9 seconds range. This is quite expected given their similar underlying structures. However, it is noteworthy that the LSTM model exhibited slightly lower prediction times for several attack types, demonstrating its effectiveness in sequential data handling. The methods proposed by Mnahi Alqahtani et al, Guosheng Zhao et al, SHAHID LATIF et al, ABDULRAHMAN AL-ABASSI et al, and Abdur Rehman Khan et al also performed similarly, exhibiting comparable prediction times. The observed variations in prediction times indicate the varying suitability of different methods for different types of attacks. It underscores the importance of understanding the characteristics of each attack type and choosing the right model accordingly. Overall, the proposed method, with its consistently lower prediction times, holds considerable promise for enhancing the speed and efficiency of cyberattack detection systems.

4.6 Discussion

The primary purpose of this research was to present a comprehensive method for detecting and preventing cyber-attacks on Industrial Internet of Things (IIoT) systems. As IIoT devices often operate with constraints on processing power and storage, implementing resource-heavy machine learning models on them can be challenging. To tackle this issue, we proposed an improved lightweight MobileNet model integrated with an Adaptive Recursive Feature Elimination (ARFE) strategy for efficient feature selection.

Our proposed method comprises two primary components: data pre-processing and feature extraction using a modified lightweight MobileNet model. During the data pre-processing stage, we normalized data to fit within a specific range, thereby ensuring the model operates on a consistent scale. We also applied outlier removal, a process of identifying and discarding data points significantly different from others in the dataset. This two-step process guarantees that the model is trained on clean, reliable, and representative data, crucial for the effectiveness of cyber-attack detection.

The second phase of our approach involves a modified lightweight MobileNet model for feature extraction. This model, originally designed for mobile and embedded applications, provides an excellent solution for resource-constrained IIoT devices due to its computational efficiency. We tailored the MobileNet's depth and width to balance between computational efficiency and predictive accuracy, ensuring the model's agility while maintaining the ability to learn complex features to distinguish between different types of cyber-attacks. This balance is crucial for a real-world deployment where resources are limited, yet high predictive accuracy is non-negotiable.

In addition to the MobileNet model, the ARFE strategy for feature selection enhances the model's predictive performance. When applied to mobile network architectures like MobileNet, the ARFE algorithm proves to be particularly effective. MobileNet architectures are designed to be computationally efficient to suit the limited resources of IIoT devices. ARFE, with its adaptive feature elimination and performance-based convergence, aligns perfectly with this efficiency mandate. The algorithm also able to handling high-dimensional data, a common attribute of IIoT datasets, effectively narrowing down the most relevant features. This is critical for building robust models capable of detecting cyber-attacks, a necessity in IIoT frameworks.

Additionally, the capability of ARFE to capture non-linear relationships among features is particularly advantageous for detecting complex cyber-attack patterns that might not be easily discernible through linear methods. Given that IIoT environments often require models to adapt in real-time to rapidly changing conditions, the inherent adaptivity of ARFE makes it an ideal choice for such dynamic scenarios. Overall, ARFE offers a comprehensive, efficient, and robust feature selection method that is highly suited for complex and resource-constrained environments like IIoT, especially when using MobileNet architectures for cyber-attack detection..

We trained and validated our model using six diverse, real-world IIoT datasets, which encompass a wide array of cyber-attack scenarios, ensuring the model's applicability across various contexts. The rigorous quantitative results indicate that our proposed method exhibits superior performance in terms of detection rate. It outperforms traditional models and methods, highlighting the advantage of combining lightweight deep learning models with adaptive feature selection.

Overall results shows, our research contributes a novel, comprehensive, and efficient approach to detecting and predicting cyber-attacks on IIoT systems. The proposed method's efficiency and robustness make it an attractive solution for real-world deployment, specifically within resource-constrained IIoT devices. The future of this research could entail refining the model further, incorporating more advanced features for improved attack detection, and broadening its application in various industrial IoT scenarios to help protect critical infrastructure from evolving cyber threats.

4. Conclusion

In this research, we addressed the increasing concern of cyber threats and breaches targeting the Industrial Internet of Things (IIoT) by proposing a comprehensive and efficient cyber-attack detection method. The strategy involves a pre-processing step to ensure data quality and a lightweight, modified MobileNet model for feature extraction, integrated with an Adaptive Recursive Feature Elimination (ARFE) strategy for effective feature selection. The proposed method proves to be both resource-efficient and accurate, making it ideal for deployment on resource-constrained IIoT devices. Our approach's robustness was tested and confirmed by training and validating the model on six diverse, real-world IIoT datasets. It demonstrated superior performance in terms of detection rate when compared to traditional models and methods. This study contributes significantly to the field by demonstrating how lightweight deep learning models combined with adaptive feature selection can help enhance cyber-attack detection in IIoT systems.

Looking ahead, we acknowledge the rapid evolution of both cyber threats and the IIoT ecosystem. Thus, we emphasize the importance of continuous refinement and adaptation of our model to meet changing requirements and new attack strategies. We hope that the foundation laid by this research can be built upon to develop even more advanced, comprehensive, and efficient cyber-attack detection methods, ultimately making the digital world safer for IIoT applications.

REFERENCES

1. Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Rajiv Suman, Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT), Sensors International, Volume 2, 2021, 100129, ISSN 2666-3511, https://doi.org/10.1016/j.sintl.2021.100129.
2. Kalsoom, T.; Ahmed, S.; Rafi-ul-Shan, P.M.; Azmat, M.; Akhtar, P.; Pervez, Z.; Imran, M.A.; Ur-Rehman, M. Impact of IoT on Manufacturing Industry 4.0: A New Triangular Systematic Review. Sustainability 2021, 13, 12506. https://doi.org/10.3390/su132212506.
3. Padhi, P.K.; Charrua-Santos, F. 6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework. Appl. Syst. Innov. 2021, 4, 11. https://doi.org/10.3390/asi4010011.
4. Pandey, N.K., Kumar, K., Saini, G. et al. Security issues and challenges in cloud of things-based applications for industrial automation. Ann Oper Res (2023). https://doi.org/10.1007/s10479-023-05285-7.
5. Dhirani LL, Armstrong E, Newe T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors (Basel). 2021 Jun 5;21(11):3901. doi: 10.3390/s21113901. PMID: 34198727; PMCID: PMC8200965.
6. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117. https://doi.org/10.3390/s23084117.
7. Cremer, F., Sheehan, B., Fortmann, M. *et al.* Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract* **47**, 698–736 (2022). https://doi.org/10.1057/s41288-022-00266-6.
8. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.
9. Tariq U, Ahmed I, Bashir AK, Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors (Basel). 2023 Apr 19;23(8):4117. doi: 10.3390/s23084117. PMID: 37112457; PMCID: PMC10142206.
10. H. Sarjan, A. Ameli and M. Ghafouri, "Cyber-Security of Industrial Internet of Things in Electric Power Systems," in IEEE Access, vol. 10, pp. 92390-92409, 2022, doi: 10.1109/ACCESS.2022.3202914.
11. S. Zeadally, E. Adi, Z. Baig and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," in *IEEE Access*, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
12. S. Zaman *et al.*, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," in *IEEE Access*, vol. 9, pp. 94668-94690, 2021, doi: 10.1109/ACCESS.2021.3089681.
13. K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in *IEEE Access*, vol. 8, pp. 222310-222354, 2020, doi: 10.1109/ACCESS.2020.3041951.
14. Alajlan, N.N.; Ibrahim, D.M. TinyML: Enabling of Inference Deep Learning Models on Ultra-Low-Power IoT Edge Devices for AI Applications. *Micromachines* **2022**, *13*, 851. https://doi.org/10.3390/mi13060851.
15. Anna Triantafyllou, Panagiotis Sarigiannidis, Thomas D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends", *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5349894, 24 pages, 2018. https://doi.org/10.1155/2018/5349894.
16. Alqahtani M, Mathkour H, Ben Ismail MM. IoT Botnet Attack Detection Based on Optimized Extreme Gradient Boosting and Feature Selection. Sensors (Basel). 2020 Nov 6;20(21):6336. doi: 10.3390/s20216336. PMID: 33172023; PMCID: PMC7664261.
17. Guosheng Zhao, Yang Wang, Jian Wang, "Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud-Fog Computing", *Security and Communication Networks*, vol. 2023, Article ID 7107663, 16 pages, 2023. https://doi.org/10.1155/2023/7107663.
18. S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network," in *IEEE Access*, vol. 8, pp. 89337-89350, 2020, doi: 10.1109/ACCESS.2020.2994079.
19. A. Al-Abassi, H. Karimipour, A. Dehghantanha and R. M. Parizi, "An Ensemble Deep Learning-Based

Cyber-Attack Detection in Industrial Control System," in *IEEE Access*, vol. 8, pp. 83965-83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

20. M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security," in *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 273-287, September 2023, doi: 10.26599/BDMA.2022.9020032.
21. Khan, A.R.; Yasin, A.; Usman, S.M.; Hussain, S.; Khalid, S.; Ullah, S.S. Exploring Lightweight Deep Learning Solution for Malware Detection in IoT Constraint Environment. *Electronics* **2022**, *11*, 4147. https://doi.org/10.3390/electronics11244147.
22. L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng and Y. Li, "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method," in *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2219-2230, 1 Oct.-Dec. 2020, doi: 10.1109/TNSE.2020.2990984.
23. Almaiah, M.A.; Ali, A.; Hajjej, F.; Pasha, M.F.; Alohali, M.A. A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Sensors* **2022**, *22*, 2112. https://doi.org/10.3390/s22062112.
24. Asesh, A. (2022). Normalization and Bias in Time Series Data. In: Biele, C., Kacprzyk, J., Kopeć, W., Owsiński, J.W., Romanowski, A., Sikorski, M. (eds) Digital Interaction and Machine Intelligence. MIDI 2021. Lecture Notes in Networks and Systems, vol 440. Springer, Cham. https://doi.org/10.1007/978-3-031-11432-8_8.
25. Salgado, C.M., Azevedo, C., Proença, H., Vieira, S.M. (2016). Noise Versus Outliers. In: Secondary Analysis of Electronic Health Records. Springer, Cham. https://doi.org/10.1007/978-3-319-43742-2_14.
26. ur Rehman, A., Belhaouari, S.B. Unsupervised outlier detection in multidimensional data. J Big Data 8, 80 (2021). https://doi.org/10.1186/s40537-021-00469-z.
27. Y. Wang, J. Yan, Q. Sun, J. Li and Z. Yang, "A MobileNets Convolutional Neural Network for GIS Partial Discharge Pattern Recognition in the Ubiquitous Power Internet of Things Context: Optimization, Comparison, and Application," in *IEEE Access*, vol. 7, pp. 150226-150236, 2019, doi: 10.1109/ACCESS.2019.2946662.
28. S. Bi, Y. Zhang, M. Dong and H. Min, "An Embedded Inference Framework for Convolutional Neural Network Applications," in IEEE Access, vol. 7, pp. 171084-171094, 2019, doi: 10.1109/ACCESS.2019.2956080.
29. K. Tange, M. De Donno, X. Fafoutis and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489-2520, Fourthquarter 2020, doi: 10.1109/COMST.2020.3011208.
30. L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye and L. Zhijun, "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 299-303, doi: 10.1109/SEGE.2019.8859773.
31. T. Elmasri, N. Samir, M. Mashaly and Y. Atef, "Evaluation of CICIDS2017 with Qualitative Comparison of Machine Learning Algorithm," 2020 IEEE Cloud Summit, Harrisburg, PA, USA, 2020, pp. 46-51, doi: 10.1109/IEEECloudSummit48914.2020.00013.
32. A. Verma and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777504.
33. Y. Meidan et al., "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," in IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, Jul.-Sep. 2018, doi: 10.1109/MPRV.2018.03367731.
34. T. Su, H. Sun, J. Zhu, S. Wang and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," in IEEE Access, vol. 8, pp. 29575-29585, 2020, doi: 10.1109/ACCESS.2020.2972627.
35. M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022, doi: 10.1109/ACCESS.2021.3137201.