Journal Pre-proof

A Cognitive Security Framework for Detecting Intrusions in IoT and 5G Utilizing Deep Learning

Umesh Kumar Lilhore , Surjeet Dalal , Sarita Simaiya

PII: S0167-4048(23)00470-4
DOI: https://doi.org/10.1016/j.cose.2023.103560
Reference: COSE 103560

To appear in: *Computers & Security*

Received date: 9 September 2023
Revised date: 17 October 2023
Accepted date: 21 October 2023

Please cite this article as: Umesh Kumar Lilhore , Surjeet Dalal , Sarita Simaiya , A Cognitive Security Framework for Detecting Intrusions in IoT and 5G Utilizing Deep Learning, *Computers & Security* (2023), doi: https://doi.org/10.1016/j.cose.2023.103560

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2023 Published by Elsevier Ltd.

Journal Pre-proof

A Cognitive Security Framework for Detecting Intrusions in IoT and 5G Utilizing Deep Learning

Umesh Kumar Lilhore[1], Surjeet Dalal[2*], Sarita Simaiya[3]

[1]Department of Computer Science & Engineering, Chandigarh University, Gharuan, Mohali, Punjab, India 140413, umeshlilhore@gmail.com

[2]Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India; profsurjeetdalal@gmail.com

[3]Apex Institute of Technology (CSE), Chandigarh University, Gharuan, Mohali, Punjab, India 140413, saritasimaiya@gmail.com

*Correspondence: Surjeet Dalal; profsurjeetdalal@gmail.com

Abstract

The fast growth of Internet of Things (IoT) gadgets and 5G networks has increased linkage and accessibility. However, growing interconnectivity poses new threat levels in these environments, making intrusion detection critical. In this article, we introduce a novel security framework that centres on deep learning and is tailored to support the particular risks posed by IoT channels and 5G networks. Deep neural networks are used in our proposed framework to effectively analyze network activity patterns and recognize any possible breaches in real-time communication. Deep learning autonomously learns complicated features and patterns, facilitating the proposed model's adaptability to changing threat vectors and traffic features. This research proposed a Hybrid model using enhanced light-weight CNNs architecture (MobileNetV3-SVM) and Transfer learning (TL) for intrusion detection in 5G communication. The proposed model utilizes the advantages of a multi-layered structure, which enables it to acquire knowledge from raw network information hierarchically. It provides the ability to distinguish between authentic and malicious behaviour efficiently. We have implemented several cutting-edge strategies to maximize the effectiveness of intrusion detection in environments characterized by limited availability of resources, such as those associated with the IoT and high-speed 5G networks. The proposed hybrid model processes network packets in real-time using light-weight MobileNet, reducing the computational overhead and making it suitable for IoT and 5G edge devices. In the proposed model, a MobileNetV3-SVM auto-classifies the network's intrusion images, enhancing the overall accuracy. In addition, to address the issue of limited labelled data in dynamic and constantly changing systems, we use a transfer learning strategy to deal with this issue. The proposed hybrid model and existing CNN-architectures, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net, are tested on CICIDS-2017, 2018 and UNSW-NB15 IoT 5G security datasets. During the experimental assessment, we demonstrated the strength of the proposed model by simulating a wide range of network settings and intrusion scenarios. Experimental findings show considerable improvements by the proposed hybrid model in accuracy, precision, false positive rates, Matthew's Correlation Coefficient (MCC) and AUC-ROC over existing approaches.

Keywords: Intrusion detection system, MobilenetV3, deep learning, 5G security, IoT, Transfer learning

1. Introduction

5G technology is the next level of wireless communication, succeeding both previous generations as the most prevalent one in the industry. We are confronted with the ever-improving advancements necessary to keep us moving further since the time we live has grown, and it grows to work quicker and more adaptable with the appliances of now. The data transfer rates of 5G networks could potentially be increased [1]. The potential for more and better intelligent items to revolutionize our quality of life

Journal Pre-proof

includes self-driving automobiles, intelligent roads, smart lights, increased Internet access provision in cities, and enhanced living standards. The intrusion detection system, or IDS, is an authentication system created to identify and cater to any violations of security and threats in the framework of 5G networks. The basic function of an intrusion IDS is to continuously track network activity and system operations to detect abnormal or malicious activity and then immediately inform system administrators [2].

The IoT and 5G connections have converged, ushering in unprecedented connectivity and game-changing technological developments. This combination holds the potential for streamlined communication, enormous data transfer rates, and the actualization of various applications, including smart cities and self-driving automobiles. The IoT devices, which are frequently characterized by their limited resource availability and heterogeneity, along with the low latency and fast data rates obtainable through 5G connections, have completely transformed how we as a species communicate with our digital surroundings [3]. However, as a result of this improved connectivity, they are now vulnerable to a wide variety of advanced cyber threats, such as initiatives at intrusion, data theft, and denial-of-service (DoS) attacks. Assuring the confidentiality and safety of IoT and 5G connections has become an urgent priority, which calls for creating highly sophisticated and adaptable systems for detecting intrusions. Objects that are part of the Internet of Things can have a wide variety of hardware standards, software platforms, and protocols for communication. These devices frequently have limited resource access, restricting their processing energy and storage capacity. Due to the heterogeneous features of connected objects and the different types of IoT gadgets, detecting intrusions faces several unique challenges. These challenges require flexible models to deal with variability in information sources and design patterns [4].

1.1 IoT -5G Architecture

IoT-5G architectural design is created to meet the needs of an extensively linked and highly data-intensive globe. It makes possible a vast array of applications that profit from fast, low-latency communication and the capacity to manage a huge number of devices at once. Since 5G was built from the bottom up, networking operations are broken down by service. The 5G fundamental "Service-Based Architecture" (SBA) is another name for this architecture for this reason [5]. Figure 1 presents the 5G network topology architecture and essential elements of a core network.

- User Equipment (UE) includes smartphones with 5G capabilities and cellular devices. IoT connects to the 5G fundamental and then to Data Networks (DN), such as the internet, via the 5G Next-generation Radio Access Network (RAN).
- Access and Mobility Management Function (AMF): The UE connection is utilized by AMF as the sole point of entry. The AMF chooses the appropriate "Session Management Function" (SMF) to supervise the user training based on the feature that the UE has requested.
- User Plane Function" (UPF): The UE and outside networks are connected by the UPF, which carries IP data throughout the network.

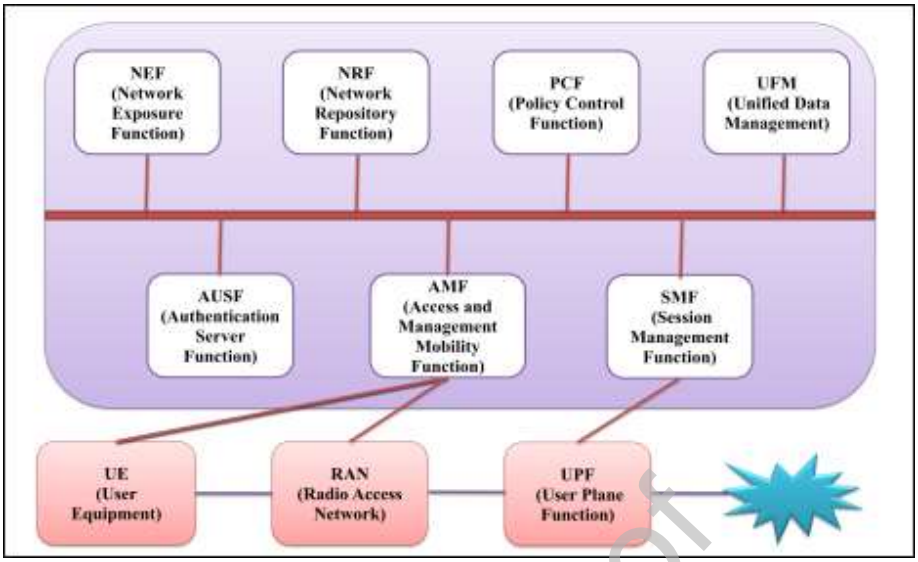


Figure 1: 5G Architecture

- Authentication Server Function (AUSF) The AMF can authenticate the UE to utilize 5G fundamental services owing to the "Authentication Server Function" (AUSF).
- The policy and permission control structure, which applies decisions regarding policy and accesses the membership information, can be obtained by other functions such as the "Session Management Function" (SMF), the "Policy Control Function" (PCF), the 'Application Function" (AF), and the "Unified Data Management' (UDM) function [6].

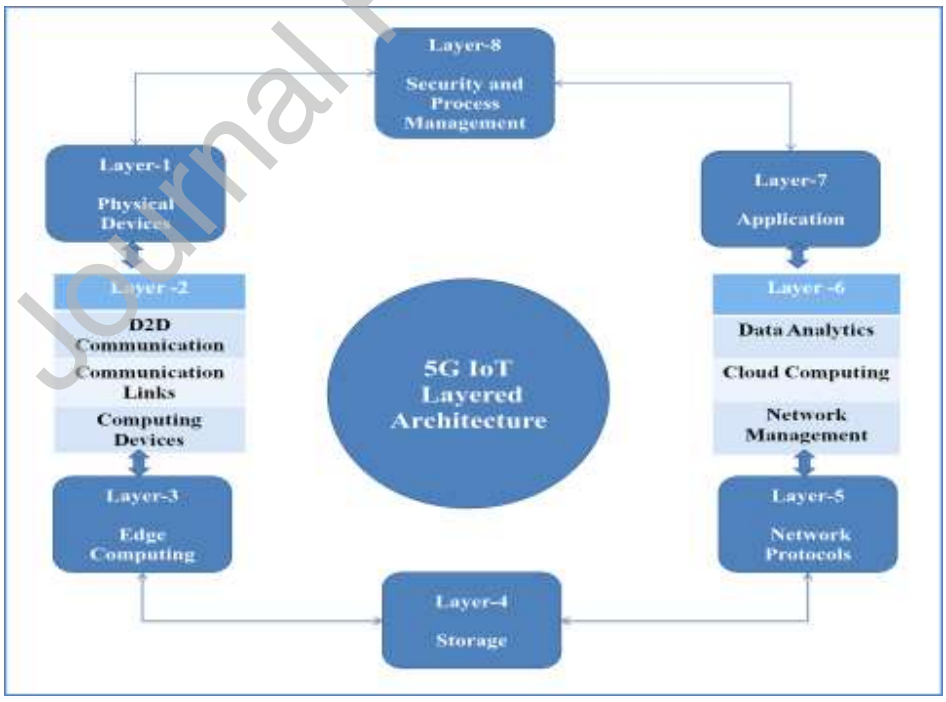


Figure 2: IoT 5G Architecture

Journal Pre-proof

Journal Pre-proof

Figure 2 presents IoT-5G architecture. This architecture is divided into 8 Layers, which cover physical devices and layer-1, device-to-device communication, links, and computing; Layer 2, edge computing at Layer 3; storage at Layer 4; network communication protocols at Layer 5; and data analytics and cloud network management at layers 6, application at layer 7 and security and process management at layer 8.

1.2 Research Question

Conventional IDS have proven to have limitations when effectively addressing the ever-changing threat landscape of environments that use IoT and 5G networks. The fact that many of the existing solutions are based on predefined rules or signatures makes them incapable of detecting novel and zero-day attacks. In addition, the real-time processing requirements of high-speed 5G networks and the limited computational resources of IoT devices have resulted in the necessity for more effective and scalable intrusion detection methods [7]. In IDS, deep learning has emerged as a potentially fruitful strategy for enhancing the safety of IoT and 5G networks. Deep neural networks can automatically learn complex features and patterns from raw data, enabling them to detect known and unknown attack patterns. This is a significant advantage for cybersecurity. By leveraging multi-layer architectures, deep learning models can capture intricate relationships within network traffic data. This leads to higher accuracy in identifying malicious activities while minimizing the number of false positives generated. One of the issues when building an intrusion detection system for 5G and IoT communication systems is the limited amount of labelled information particular to this field. Transfer learning enables a model to train a baseline using pre-existing labelled information from related domain names, such as conventional wired networks of wireless networks similar to 4G [8].

1.3 Key Contribution

This article presents a hybrid security model based on light-weight CNN and Transfer learning. It is designed to deal with the particular obstacles created by IoT and 5G connections [9].

- The proposed model is based on light-weight CNN (MobilenetV3 with SVM) and transfer learning to solve the problem of limited labelled data in both the Internet of Things and the 5G context. This strategy uses the knowledge gained from more extensive datasets, enabling the model to effectively generalize and detect intrusions, even when only a few labelled samples are available.
- The proposed model also utilizes a decision tree to prioritize the distinct network flow measures or features to acquire various threats.
- The proposed model takes advantage of the benefits offered by deep neural networks, which enables it to learn in an adaptable manner from the ever-changing paths of attack along with network traffic.
- We have optimized the structure of the model for performance and processing in real-time so that it can be used in Internet of Things devices with limited resources and high-speed 5G wireless networks. It mainly ensures that the model is applicable in both contexts.
- We prove the better accuracy of the proposed deep learning-driven security framework compared to other intrusion detection approaches by conducting an exhaustive exploratory test and comparing the results to the benchmark datasets, i.e., CICIDS-2017, 2018 and UNSW-NB15 IoT datasets.
- Our proposed approach involves transforming a network flow pattern occurring within a defined time through a two-dimensional structure image. The image consists of two dimensions: one indicates the different measures of the network flow (known as features), while the additional dimension indicates the data of those measures as they change over time. Subsequently, we employ image processing methodologies to separate these factors images as benign or malicious classes.

Journal Pre-proof

- The SoftMax classifier normally employed in CNNs is being replaced with a support vector machine (SVM) classifier to strengthen the resilience of IDS classification. The hinged loss function utilized by the SVM is employed to back-propagate a CNN model to enhance the prediction accuracy of the classifier on the IDS dataset, which eliminates overfitting and enhances the classification outcomes.

The findings highlight the model's effectiveness in managing real-time traffic, its capacity to adapt to ever-changing attack strategies, and its capacity to protect IoT and 5G networks against various cyber threats. This investigation helps promote the advancement of cutting-edge intrusion detection systems that can preserve the confidentiality and dependability of modern interrelated ecological systems by integrating the strength of deep learning alongside the complexities of the Internet of Things and 5G privacy concerns.

1.5 Organization of the article

The complete article is organized in various sections. Section two covers the related work of existing Intrusion detection systems using machine learning and deep learning. Section three covers material and methods; we explain the technical aspects of the proposed security framework, including its architecture and technique; section four covers results and discussion in which we cover experiment setup and outcome measurements; section five explains the conclusion and future work.

2. Related Works

Deep learning algorithms have been suggested as a potential solution for detecting intrusions in the context of the IoT and 5G networks, aiming to mitigate the cybersecurity issues associated with these networks. These models provide a methodology that utilizes data-driven techniques to identify and mitigate emerging and previously unidentified attacks. The proposed algorithms encompass an enhanced deep reinforcement learning (DRL) structure incorporating parameter tuning through IoT examines [10]. A Temporal Convolution Neural Network (TCNN) is also introduced, amalgamating CNN and generic convolution techniques for IDS in the IoT domain [11]. Lastly, an intrusion detection system that uses deep learning has been suggested for a multiple cloud IoT ecology, aiming to enhance both the precision of detection and instruction efficiency [12]. Furthermore, a proposed collaborative learning framework has suggested the utilization of TL to enhance the effectiveness of online attack detection systems in Internet of Things networks. This framework addresses challenges, including the lack of labelled data and the variance of data characteristics [13]. As mentioned earlier, the methodologies showcase the capacity of deep learning to augment intrusion detection capabilities within the Internet of Things and 5G technologies.

The bandwidth, capacities, and stability required by IoT gadgets and their corresponding applications are provided by 5G, which closely relates to networks used by IoT devices. However, such networks' safety and privacy are significant areas of apprehension. Risk management strategies are crucial in safeguarding sensitive data and mitigating cyber-attack occurrence [14]. A deep learning-based security solution is discussed to enhance the safety, confidentiality and protection of IoT devices running within 5G networks. It is imperative to implement customized security solutions encompassing authentication, encryption and information ethical conduct mechanisms [15]. Furthermore, incorporating cryptographic techniques and quantum technology can potentially augment data security within 5G networks [16]. Integrating 5G and IoT networks facilitates the implementation of diverse applications, including smart

Journal Pre-proof

cities, wearable sensors, and various IoT use cases. However, ensuring the security of these networks is crucial in mitigating potential risks, including DDoS attacks [17].

Artificial intelligence methodologies can be utilized to estimate traffic load and optimize access schemes within cellular networks, thereby facilitating the effective operation of IoT devices in the context of 5G networks [18]. The utilization of deep learning and machine learning methodologies is currently being investigated to augment the security measures implemented in 5G networks. These networks encounter various security challenges, such as tampering with authentication and authorization, masquerade and robot attempts, and vulnerabilities in the source files [19]. The use of adversarial machine learning techniques in attacks against communication networks in 5G infrastructure poses a significant risk, particularly to sharing spectrum and physical layer authorization [20]. The adoption of software-defined services in 5G systems has rendered them susceptible to security risks, thus requiring the development of a comprehensive framework for analyzing their security. The utilization of machine learning techniques enables the examination of attack graphs, facilitating the detection of potential exploits and flaws within the basic network of 5G [21]. Machine learning and deep learning models can be utilized to mitigate ransomware, malware, and other malicious attacks within 5G networks and the forthcoming 6G networks [22].

Furthermore, incorporating Blockchain, machine learning, and other technologies can potentially augment security measures and safeguard privacy in 5G and further [23].To protect against hacking attempts, detection systems for intrusions are now required due to the integration of cyber-physical systems (CPS) along with the IoT. On the other hand, the training of IDS in resulting CPS disciplines is sometimes difficult due to skewed and missing data sets [24]. A generative adversarial network, a GAN-based intrusion detection system (G-IDS), was offered to solve this problem. G-IDS use GAN to generate artificial specimens, which can be used to train the IDS in conjunction with the real samples. This method is superior to standalone IDS models [25], as it enhances the identification of attacks and model stabilization while being trained. Additionally, to obtain high-level features from large amounts of data, algorithms using machine learning that include supervised learning were utilized to implement IDS for Internet of Things systems [26]. Table 1 presents a comparative analysis of various IDS detection methods in IoT and 5G communication systems.

Table 1: Comparison of existing IDS detection techniques

References	Method Used	Source-based Dataset	Target based dataset	Precision
[11]	CNN model	NSL-KDD	NSL-KDD	86.34%
[12]	DNN model	UNSW-NB15	NSL-KDD	80.67%
[13]	KNN-PCA method	DoS with Normal	R2L with Normal	86.35%
[14]	RF-SVM method	AWID dataset	AWID dataset	90.26%
[15]	CNN	CICIDS2017	Custom dataset	88.35%
[16]	Bit-Efficient Net Model	CICIDS-2017	Custom dataset	90.24%
[17]	CNN-CNN	BoT (Botnets traffic) and IoT	TON with IoT	89.65%
[18]	DNN	CICIDS2017	Custom dataset	83.24%
[19]	CNN-TL	CICIDS2017 and UNSW-NB15	Custom dataset	91.23% and 90.54 %

Proposed Hybrid model	Hybrid Light-weight CNN (MobileNetV3-SVM and Transfer Learning)	CICIDS-2017 and 2018 datasets	Custom dataset	98.25% and 96.54%

3. Materials and Methods

This section covers the materials and methods related to the IDS research.

3.1 Dataset

This research utilizes the online IoT 5G dataset; the details of the dataset are as follows.

- **UNSW-NB15 IoT dataset:** A renowned dataset of IoT and 5G network traffic called "UNSW-NB15 IoT Dataset" includes a variety of network traffic instances. It was developed to analyze network security issues and perform tests on various systems to detect intrusions. Although the dataset does not solely concentrate on IoT research, it offers knowledge about various attacks and network behaviours, making it a tremendous help for researchers working on security measures [21]. This data collection includes 175341 rows, each with a different 45 attributes. Figure 3 presents attack categories in the UNSW-NB15 IoT dataset.

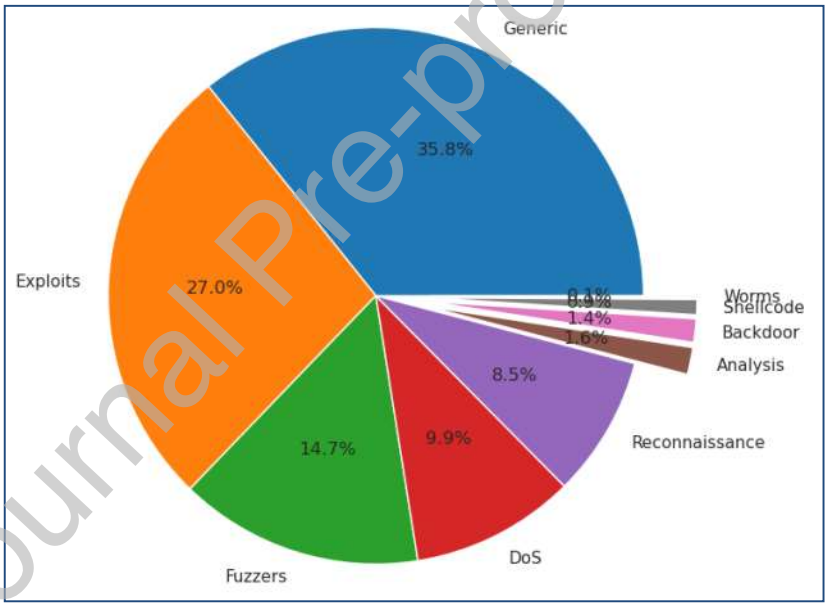


Figure 3: Attack categories in the UNSW-NB15 IoT dataset

- **CICIDS-2017:** The "Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset 2017", also known as CICIDS-2017, is an extensive cybersecurity dataset created to study and assess intrusion detection and prevention systems. It was developed to simplify developing and testing techniques and models to identify and lessen online attacks. The dataset includes network traffic information created in a controlled setting to represent typical network operations and different malware infections [22]. Figure 4 presents the attack count of the CICIDS-2017 dataset.

Journal Pre-proof

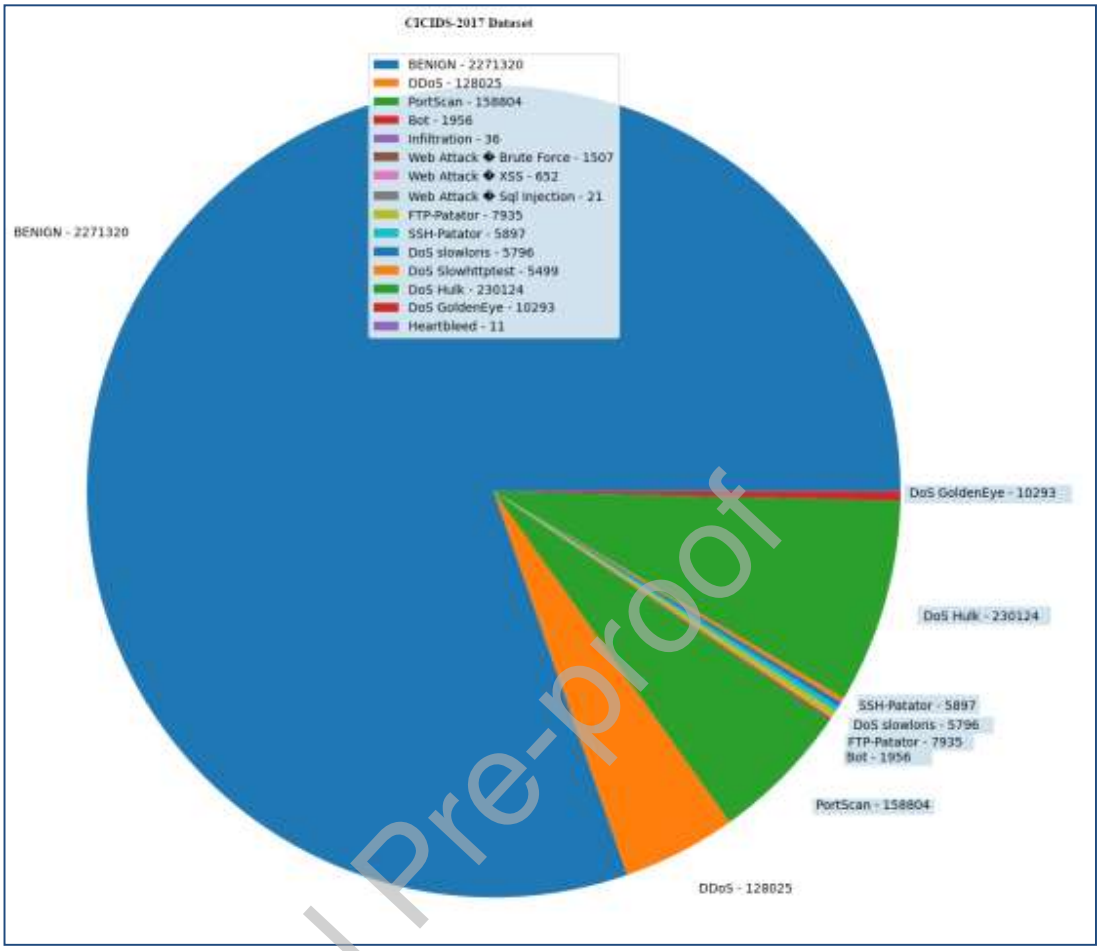


Figure 4: Attack count in the CICIDS-2017 dataset

- **CICIDS-2018:** The Canadian Institute for Cybersecurity (CIC) and the Communications Security Establishment (CSE) collaborated on this dataset-generation venture, which uses the idea of individuals to create cybersecurity datasets methodically. It includes an in-depth explanation of intrusions and generic distribution frameworks for applications, procedures, and lower-level structure entities. The dataset contains seven distinct attack instances, including 'brute force', 'heart-bleed', 'botnets', 'denial-of-service', 'distributed denial-of-service, 'web attacks', and 'network infiltration'. The total count includes Benign 667626, FTP-Brute-Force 193360 and SSH-Brute-force 187589 [23]. Figure 5 presents the attack count in the CICIDS-2018 dataset.

Journal Pre-proof

Journal Pre-proof

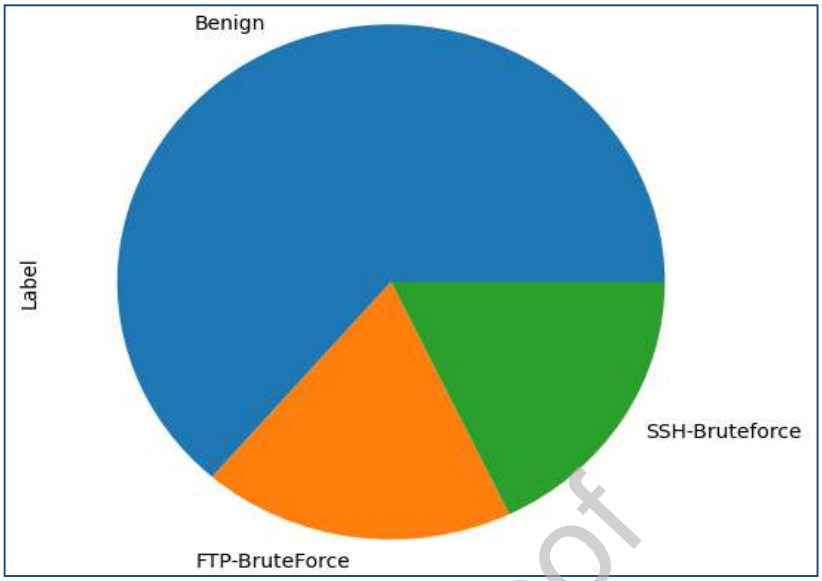


Figure 5: Attack count in the CICIDS-2018 dataset

3.2 Data Pre-processing

Data pre-processing has become important when interacting with data sets, i.e., CICIDS-2017, 2018 and UNSW-NB15 IoT 5G security datasets. All three datasets are in CSV file format. In the dataset CSV file, every row indicates an individual network flow, whereas each column denotes a distinct network attribute. Data pre-processing includes data cleaning, transforming, and organizing the data. Preparing the dataset for further processing, such as data analysis and modelling, is more important. Preprocessing the IoT IDS database includes retrieving the information coming from the source, analyzing its organizational structure, and managing any missing values, involving outlier detection. The categorical factors are then encoded into numbers, and the numerical attributes are converted into a fairly standard range. The oversampling and under-sampling strategies remove the class imbalance problem in the IDS datasets.

3.2.1 Important Features extraction

This phase involves the selection of important features from each of the IDS datasets. Each row represents a network flow in the CSV file, and a specific network feature is represented by each column. A decision tree (DT) classification method is utilized to ascertain the essential characteristics for determining attack classes from IDS datasets. DT selects the most significant attributes for each specific category of attack. To enhance the preciseness of the DT, we employed the MDOM (Mahalanobis Distance-based Oversampling Method) to level off the distance concern from each attack class. MDOM is a method of oversampling that utilizes a Mahalanobis distance to create artificial samples. This distant metric considers the distribution and correlation of features within the dataset. This technique is efficient in multi-class along with multi-label algorithms for classification when dealing with an imbalance dataset during the training process.

All three datasets, i.e., CICIDS-2017, 2018 and UNSW-NB15, are in CSV file format. In the dataset CSV file, every row indicates an individual network flow, whereas each column denotes a distinct network attribute. The dataset contains information in rows and columns to provide a specific instance within the specified framework. For example, the CIC IDS2017 samples comprise 78 distinct features. This dataset has 271 rows, along with 78 columns, with 14 types of attacks. A similar CICIDS-2018

Journal Pre-proof

dataset contains 7 attack classes, 6 columns and 80 columns, and the UNSW-NB15 dataset contains 61 columns and 81,173 rows, with 9 attack classes.

3.2.2 Dataset Conversion into Images

During this step, we commence by creating an empty image with dimensions comparing the numerous pieces of columns and rows in the novel CSV file. Subsequently, every characteristic value in the novel CSV file is also transformed into an RGB value within the spectrum of (0×000000) towards (0xFFFFFF), representing a 24-bit colour. This research involves the creation of two distinct image databases. The first set is an RGB set consisting of three colour channels such as (Red, Green, and Blue). The second set is a grey scale set with only considered one channel. An RGB visual is a composite structure consisting of three colour channels, which are then transformed towards an array of pixels with dimensions (M × N × 3). M represents the variety of columns, while N represents the variety of rows. To accomplish this, first, discover the maximum and minimum possible values of every single characteristic in the IDS dataset, then attempt the most important features range to gradually map out the feature importance to the corresponding 24-bit RGB spectrum. The decimal representation of this 24-bit range spans 0 to 16777215, corresponding to a total of 16.7 million colours.

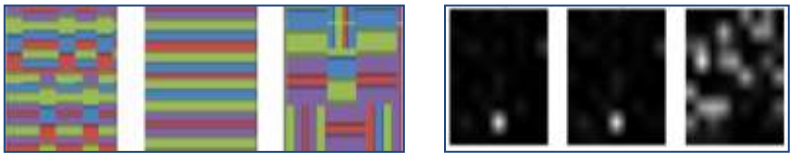
The proposed approach also transforms a network flow pattern occurring within a defined time through a two-dimensional structure image. The image consists of two dimensions: one indicates the different measures of the network flow (known as features), while the additional dimension indicates the data of those measures as they change over time. Subsequently, we employ image processing methodologies to separate these factors images as benign or malicious classes. The value of each colour portion is found in eight bits and two digits in Hexadecimal within the 24-bit RGB colour value. The first two numbers in Hexadecimal (8-bits) represent the numerical promote of the Red element. The subsequent 8 bits represent the magnitude of the Green element, while the final 8 bits correspond to the magnitude of the Blue element. We can obtain the corresponding values of each hue of the RGB colour elements by dividing the modulus division for the 24-bit significance at least twice by (0xFF) or as 256 in the decimal form.

Next, these colour elements are correctly placed in the image's RGB channel. Then, the above process is repeated for each of the chosen characteristics that were taken into account within the specified time frame and recorded in the CSV file. Based on how much a malicious activity flow is present throughout the timeframe shown in each image's rows of size (N × 24 × 3), visual receives training identifies assigned to it. The particular type of threat, if any, is used based on that image's training sign. Afterwards, we also applied an Image augmentation method to the IDS dataset. It is a technique widely employed in visual analysis along with deep neural networks to artificially increase a dataset's capacity by applying various transformations towards the primary images. This is accomplished through the application of image augmentation programs. Introducing diversity into the training data improves the accuracy of predictive models and the applicability of their results. Image augmentation is especially useful for dealing with inadequate training data and allows for being more resilient to modifications in IDS datasets. Both of these challenges can be overcome through image augmentation [24].

The utilization of this conversion technique is potentially advantageous in the application of deep learning models that are primarily designed for image data to time-series data. However, it is crucial to consider the computational cost, particularly when dealing with large data sets such as CICIDS-2017, CICIDS-2018, and UNSW-NB15. We have applied windowing, Scaling, Feature representation and

Journal Pre-proof

Stacking key strategies for image conversion. Algorithm 1 presents the steps to convert the IDS numerical data set into images. Figure 6 presents the sample images obtained from numerical IDS datasets.



(a) Colored (b)Grey Scale

Figure 6: Sample images obtained from numerical IDS datasets

//Algorithm 1: IDS numerical data conversion into images
Input: IDS numerical data in CSV
Output: IDS dataset into equivalent Images

1. Define the essential libraries, i.e., NumPy, Matplotlib, pyplot module
2. Load the CSV IoT IDS number dataset, i.e., CICIDS-2017, CICIDS-2018, and UNSW-NB15.
3. Define the essential parameters for generating an image
   Set image_width = 64
   Set image_height = 64
4. Choose a particular colour map for data visualization
   Set colorMap = "viri-dis"
5. Create a novel empty list to store images
   Set images = [ ] ;
6. Repeat steps from 6 to 11 till IDS_dataset !=' NULL';
7. Extract essential features from the IDS dataset to create equivalent images.
   Data_Imp_features = FeatureExtract(records);
8. Apply a feature Normalization on the extracted features,
   if the Feature range == [o , 1]
   Features == normalizeFeatures
   NormalizedFeature= normalizeFeatures
   Else
   Set FeatureRange= [0,1]
9. Generate an empty image
   Empty_image = np.zeros((image_height, image_width,))
10. Assign 10. Attribute numerical values to every individual pixel within the image.
    for j in range(image_width):
        repeat and set image_height by using the data variable k
11. Check weather a pixel value is equal to the normalized features.
    Multiply the variable j by (imageWidth+k)
    Reset the (pixel_value) to the new image position (j,k)

3.3 Proposed Hybrid model

The proposed hybrid security model uses light-weight CNNs (MobileNetV3-SVM) with transfer learning. Developing efficient and effective models for a wide range of activities, which includes detecting attacks

and intruders in IoT and 5G communications networks, is accomplished with the assistance of a powerful method known as a light-weight CNN combined with transfer learning. This strategy entails using the light-weight CNN architecture with some weights previously trained across a dataset of greater size, followed by fine-tuning the model's parameters using a smaller goal dataset. The method is applied to a bigger set of data first.

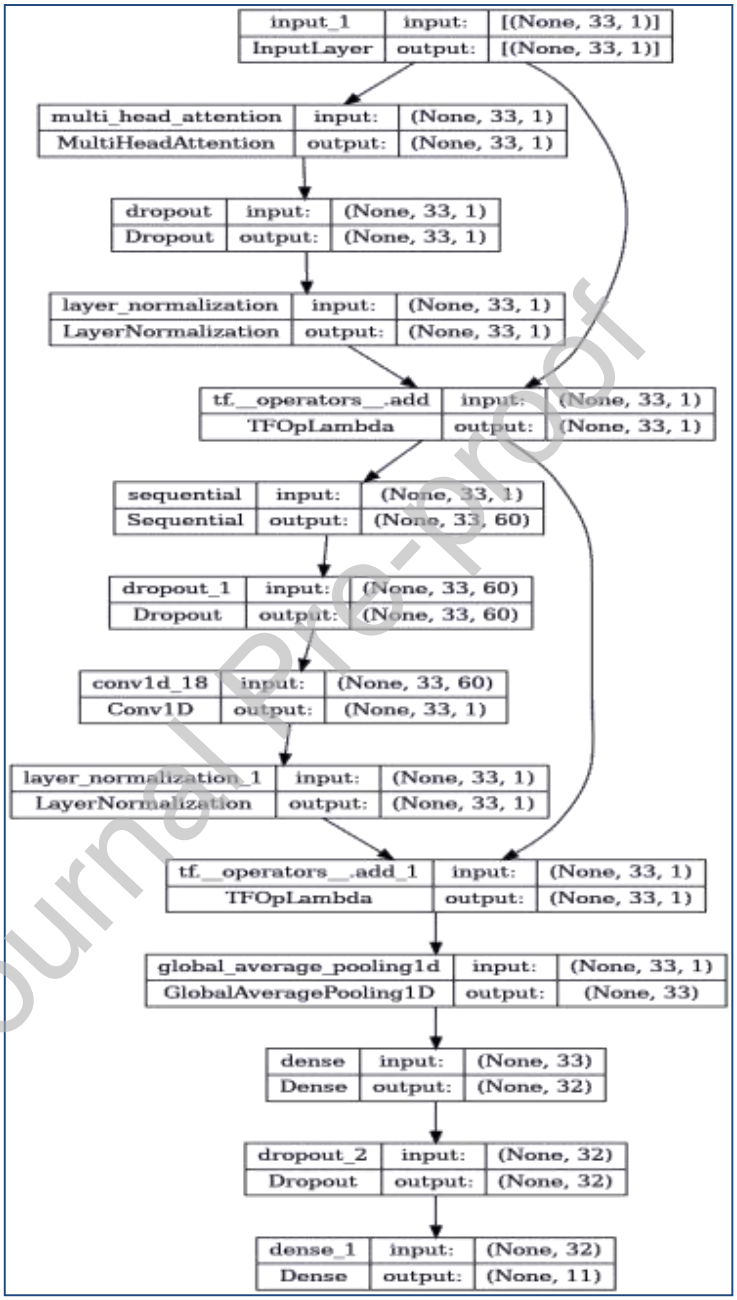


Figure 6: Structure of Proposed Hybrid Model

Figure 6 highlights the structure of the proposed hybrid model. It aims to balance the complexity of the models and computational effectiveness, making it appropriate for deployment in contexts with limited resources, such as portable electronics, smartphones, tablets, and IoT gadgets. A light-weight CNN

Journal Pre-proof

framework is developed to achieve this excellent trade-off. These architectures' primary objective is to improve intrusion detection efficiency in IoT and 5G [25]. The working steps of the proposed model are described in Figure 7.

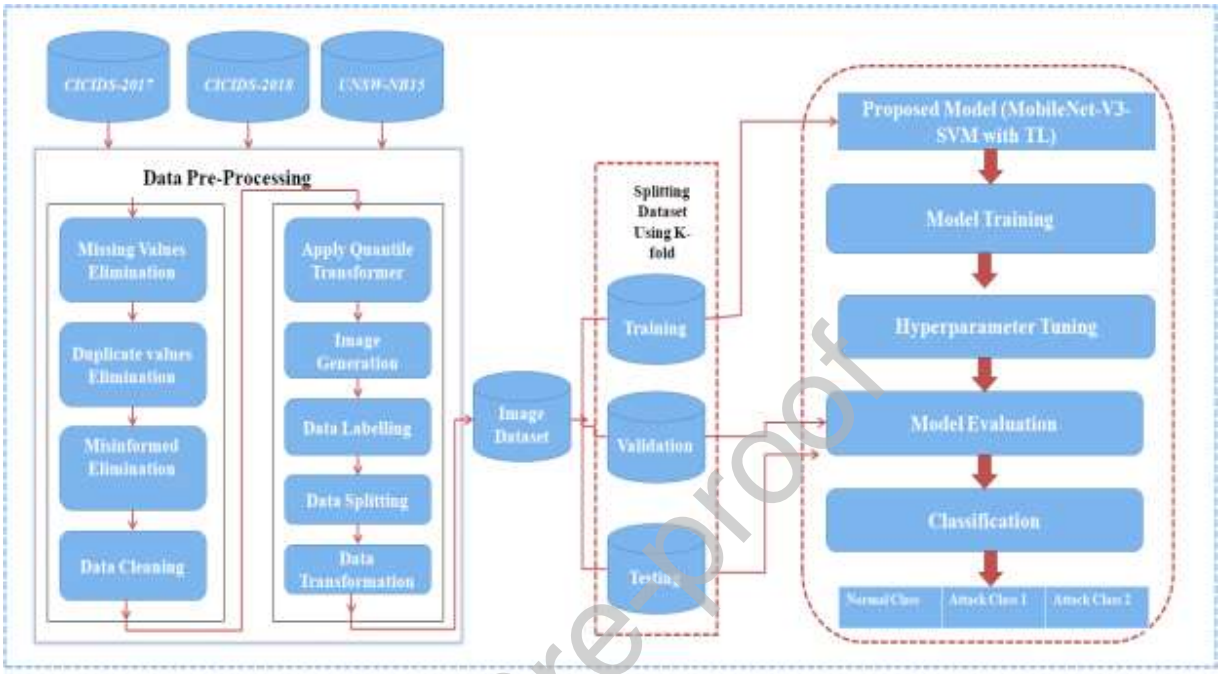


Figure 7: Working of proposed hybrid model

- **Feature Extraction (FE):** Utilize a previously trained MobileNetV3 framework for extracting features from the IDS dataset. MobileNetV3 is a light-weight CNN architecture optimized specifically for portable and embedded computing devices, i.e., IoT. It is possible to obtain high-level characteristics from visuals through network traffic communications.
- **Feature Transformation (FT) and Feature Selection (FS):** FT is based on the structure of retrieved characteristics; we applied data normalization and data transformation to satisfy the specifications of the SVM method. For FS, the proposed model also utilizes a decision tree to prioritize the distinct network flow measures (also known as features) to acquire various threats. The proposed approach also involves transforming a network flow pattern occurring within a defined period through a two-dimensional structure image. When the characteristics obtained are high-dimensional in FS, explore strategies like Principal Component Analysis (PCA) that minimize the dimension while maintaining significant details [26].
- **SVM Model Integration:** An SVM method is applied in the next phase. SVM performs the following essential jobs.
  - **Splitting dataset:** The datasets are divided into training, testing and validation ratios, i.e., 60:20:20 and 70:15:15.
  - **Training the model:** Use the obtained and transformed characteristics as the inputs for training an SVM model, along with the appropriate intrusion categories as outcomes. We implement the polynomial problems SVM kernel to deal with data with suitable features.

Journal Pre-proof

- **Tuning of Hyperparameters:** Use the obtained and transformed characteristics as the inputs for training an SVM model, along with the appropriate intrusion categories as outcomes. We implement the polynomial problems SVM kernel to deal with data with suitable features.

3.4.1 Proposed Hybrid Model Algorithm

Algorithm 2 presents the algorithm of the proposed hybrid model.

*// **Algorithm 2: Proposed Hybrid Model***
***Input:** IDS Dataset, i.e., CICIDS-2017, 2018 and UNSW-NB15*
***Output:** Intruder class*
1. Apply data Pre-processing
2. Utilises Pre-trained light-weight CNN model
 # Load a pre-trained CNN model MobileNet-V3
2.1 mobile_net_model = load_mobilenet_v3_model()
3. Feature extraction
 # Extract the essential features by applying the MobileNet_V3lightweight CNN model
3.1 training-features = mobile_net_model.prediction(training_data)
3.2 validation_features = mobile_net_model.prediction(validation_data)
3.3 testing_features = mobile_net_model.prediction(testing_data)
4. Apply Feature transformation
 # Transformation and selection of features
4.1 training_features = normalization_features(training_features)
4.2 validation_features = normalization_features(validation_features)
4.3 testing_features = normalization_features(testing_features)
5. Apply training features for the SVM model
5.1 svm_training_model = training-svm-model(training_features, training_labels)
6. Apply Hyperparameter tuning by applying SVM
6.1 Fine_tuned_svm_model =Fine_ tune_svm_hyper_parameters(validation_features, validation_labels)
7. Evaluate the performance of the SVM model on IDS datasets
7.1 Measure precision, accuracy, f1-score, recall, roc-curve = evaluatation_svm_model(testing_features, testing_labels)
8. Apply a Transfer learning model
8.1 transfer-learning_mobile_net_model = perform_transfer_learning(train_data, train_labels, mobilenet_model)
9. Applying optimization and fine-tuning of parameters by optimized SVM
9.1 optimization_svm_model = optimization_svm_hyper_parameters(validation_features, validation_labels)

3.4.2 Light-weight CNN Architecture (MobileNetV3)

To produce light-weight CNNs which perform exceptionally well in environments with limited resources, the architecture of MobileNetV3 emphasizes cutting-edge principles of design, including Inverted Residual (IR), Efficient Depthwise Separable Convolutions (EDSC), Hard-Swish Activation (HSA), SE Blocks, Architecture Variants (AV), Adaptive Global Average Pooling (AGVP) blocks. This framework is efficiently utilized for IoT and 5G connection operations, including classifying and detecting objects and intrusions. It achieves a balance between high performance and efficient computation [27].

- **Inverted Residual (IR) Blocks:** MobileNetV3 uses inverted residual blocks developed to balance computational complexity and functionality levels. These blocks are made by layering a linear projection placed on top of an intimate bottleneck layer, followed by a non-linear activation function.

Journal Pre-proof

The linear projection boosts dimensionality, allowing enhanced feature representation; the shallow bottleneck also decreases computing power [28].

- **Efficient Depthwise Separable Convolutions (EDSC):** MobileNetV3 generally uses depthwise distinct convolutions, separating the norm convolutions through depthwise and point-by-point convolutions. It lowers the amount of computation that needs to be done while maintaining the power of expression. Utilizing "hard-swish" activation functions and "squeeze-and-excitation" blocks contribute to an additional improvement in the effectiveness.
- **Hard-Swish Activation (HSA):** The activation function known as hard-swish achieves a good balance among both linear and non-linear activation events, which helps to reduce computation while simultaneously enhancing accuracy. It is built to be better suited for mobile devices and embedded environments while still maintaining a good balance between effectiveness and speed. This is due to the design of the system.
- **SE Blocks:** It can identify channel-wise interactions by utilizing a global average pooling functioning, followed by several completely linked layers. This technique allows the model to highlight significant characteristics while simultaneously suppressing less important instances adaptively.
- **Architecture Variants (AV):** There are several architecture variations offered by MobileNetV3, such as tiny and large, along with EdgeTPU variants, each of which is optimized for a particular trade-off between precision and effectiveness. The Massive variant offers superior precision at a slightly increased computational expense, while the tiny variant is lighter and more appropriate for extremely constrained situations.
- **Adaptive Global Average Pooling (AGVP):** To decrease the geographical dimensions of mappings of features while maintaining their channel-wise information, MobileNetV3 uses adaptive pooling of global averages. The effectiveness of computation gets boosted even more by this procedure.

3.4.3 Transfer Learning

The concept of transfer learning implies the exercise of retaining the knowledge gained from the procedure of addressing a situation and applying it to a subsequent instance of intrusion detection or a different problem of a similar nature. This is especially beneficial when the number of observations is small because it makes it simpler for the model to respond to novel information. If trained from beginning to end, the simulation couldn't react quickly or effectively to new data. This study's authors use models with CNN pre-training weights that are not particularly heavy. In addition to that, the model's sensitivity was adjusted through the course of this research. The step of fine-tuning contributes to the achievement of enhancements in the results produced by the model. It assumes that a model's variables must be changed precisely for the framework to react to specific circumstances [29].

During fine-tuning, a model that has been trained or an element of it is unfrozen. After that, training occurs again on the most recent data, with a shallower learning rate. As a consequence of this, the weights which were previously learned are altered to some degree. For this study, the encoder weights have been kept constant to facilitate fine-tuning. As per the author [30], there are instances in which we can stop training the encoder and instead train just the de-coder that had been randomly initialized. This is done to avoid causing damage to the weights, which were correctly trained using big gradients throughout the initial training phases. The main approach for fine-tuning (i.e., having the identical amount of data as the total amount of classes in the newly created dataset) is to take chosen pre-trained CNN structures, remove the final layer that is completely connected, and afterwards replace it with one or more of our novel fully

Journal Pre-proof

connected layers. This is done after the models have been pre-trained. The dataset contains benign and malignant attack classes in the imaging datasets, and we divided the data into two classes for this research.

3.5 Mathematical model Proposed hybrid Model

Developing a complete mathematical representation for MobileNet-V3 combined with an SVM involves outlining the conceptual framework of MobileNet-V3, laying out how to obtain parameters from it, and describing how the SVM utilizes those features with classification [31]. MobileNet-V3 serves as a CNN structure for the classification of images. It comprises depthwise distinct convolutions, which contribute to maintaining efficiency while lowering computational complexity. A Support Vector Machine is a machine learning technique employed to perform classification. It locates a hyperplane that effectively divides data points from various classes.

Let I be the set of the input image, and C_L is the set of convolution layers.

Input: *input image set.*

$$\{I\} = \{I_1, I_2, \ldots\ldots\ldots\ldots I_n\} \quad (1)$$

Output: *Once the convolutional layers have been built, F_MobileNet-V_3(I) results from the MobileNet-V_3 structures. It's an in-depth visualization of the characteristics of an input appearance.*

//Extraction of features using MobileNet-V_3

Take an input image I_1 from the input set {I}

F_MobileNet-V_3 (I) represents a feature vector retrieved using the MobileNet-V_3 model.

Employing MobileNetV3, let's refer to the retrieved feature vector as FV(X) and the input of the network communication instance as X. It is possible to visualize this transformation as follows.

$$FV(X) = F_{MobileNetV3}(X) \quad (2)$$

//Set the parameters of SVM for MobileNet-V_3

W_g represents the weight vector, b_s represents the bias, and F_v represents the feature vector.

//SVM classification decision model

SVM decision can be obtained by using equation (3).

$$ClassSet(I) = Sign[W_g \ddot{o} F_{MobileNet} - V3(I) + b_s \quad (3)$$

Here, ö returns +1 and -1 for positive and negative outcomes.

// Split the dataset d in various subsets $d_{training}$, $d_{validation}$, and $d_{testing}$

$$dataset = \{d_{training}, d_{testing}, d_{vaidation}\} \quad (4)$$

// Model Training

Perform labelling feature on the dataset by model

$$Label(I) = \{(I_1, L_1), (I_2, L_2) \ldots\ldots (I_n, L_{1n})\} \quad (6)$$

Here, I represent input, and L represents Labeled data.

// Model Testing and Validation

$$Model = \{m_{training}, m_{testing}, m_{vaidation}\} \quad (7)$$

// Combining the model F_MobileNet-V_3 with the SVM model for final output.

$$F_{output} = Combine\ (F_i, F_{MobileNetV3}(X)) \quad (8)$$

3.6 Performance Measuring Parameters

Journal Pre-proof

To measure the performance of the existing method and proposed method, the following performance measuring parameters were used [33].

3.6.1 MSE: It is called a "Mean Squared Error". The average squared variances between the actual and predicted outcomes are frequently measured using this metric, especially in regression problems, as described in Equation 9.

$$\mathrm{MSE} = (1/n) * \Sigma(\mathrm{actual}_{\mathrm{value}} - \mathrm{predicted}_{\mathrm{value}})^2 \quad (9)$$

3.6.2 RMSE: It is called "Root Mean Square Error". It is becoming more adept at evaluating the precision of a prediction model. Regression models, designed to forecast constant numerical values, are evaluated using RMSE, which proves particularly helpful in this situation, as described in equation 10.

$$\left[\mathrm{RMSE} = \sqrt{\left\{\frac{\Sigma_{\{i=1\}}^{\{n\}}(y_{\{i\}} - \{y\}_{\{i\}})^2}{N}\right\}}\right] \quad (10)$$

3.6.3 MAE: It is called a "mean absolute error ".The standard deviation absolute distinction between the actual and predicted values is measured using this metric. It is frequently used to assess how well models with regression perform, as described in equation 11.

$$\left[\mathrm{RMSE} = \sqrt{\left\{\frac{\Sigma_{\{i=1\}}^{\{n\}}(|y_{\{i\}} - x_{\{i\}}|)^2}{N}\right\}}\right] \quad (11)$$

3.6.4 Accuracy: It assesses the general accuracy of the classification algorithm's predictions. It is the proportion of instances accurately anticipated to the overall number described in equation 12.

$$\left[\mathrm{Accuracy} = \frac{\mathrm{True}_{\mathrm{Positive}} + \mathrm{True}_{\mathrm{Negative}}}{\mathrm{True}_{\mathrm{Positive}} + \mathrm{True}_{\mathrm{Negative}} + \mathrm{False}_{\mathrm{positive}} + \mathrm{False}_{\mathrm{Negative}}}\right] \quad (12)$$

3.6.5 Precision: It shows how many of an algorithm's positive forecasts genuinely come true. It's a measurement which assists in clarifying how well the model can steer clear of producing false positives, as described in equation 13.

$$\left[\mathrm{Precision} = \frac{\mathrm{True}_{\mathrm{Positive}}}{\mathrm{True}_{\mathrm{Positive}} + \mathrm{False}_{\mathrm{positive}}}\right] \quad (13)$$

3.6.6 Recall: It estimates the number of "truly positive results" that were correctly forecasted by the algorithm. It is also called "sensitivity" or the "true positive rate", as described in equation 14.

$$\left[\mathrm{Recall} = \frac{\mathrm{True}_{\mathrm{Positive}}}{\mathrm{True}_{\mathrm{Positive}} + \mathrm{False}_{\mathrm{Negative}}}\right] \quad (14)$$

3.6.7 F-Measure: In the fields of artificial intelligence and knowledge retrieval, it serves as a metric that is frequently used, and one of its other names is the F1 score. It measures the efficacy of binary classification scenarios, classifying instances through one of two classes, generally "positive" and "negative", as described in equation 15.

$$\left[\mathrm{F}_{\mathrm{Measure}} = 2 * \{\frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}}\right] \quad (13)$$

3.6.8 Confusion Matrix: The performance of a classification system is usually evaluated via the support of a confusion matrix, which is a technique. Determining how well the algorithm can categorize instances into various groups or categories is helpful. The matrix offers a concise

Journal Pre-proof

summary of the correct positive, correct negative, incorrect positive and incorrect negative predictions generated by the algorithm.

4 Simulation Results and Discussion

This section covers the simulation results computed on three benchmark IDS datasets, i.e., CICIDS-2017, 2018 and UNSW-NB15. The proposed hybrid model and existing models, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net, are implemented using Python programming language with key libraries Numpy, Keras, Sci-kit, Matplot, Pandas and tensor flow implemented and executed on a machine with hardware configurations of Core-i7, 10700 processor, CPU @ 3.7Ghz, 16GB RAM, and windows 11 OS [34].

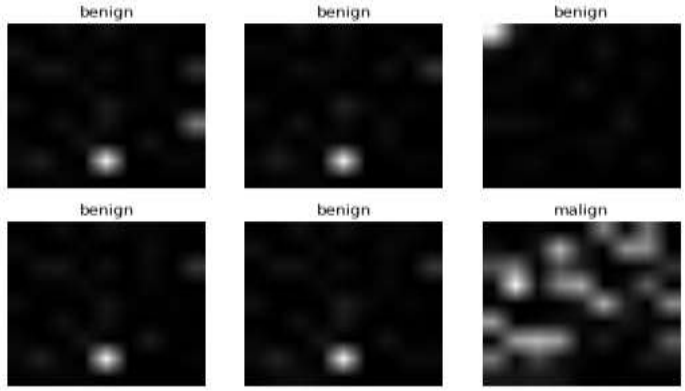
After pre-processing the dataset, all three datasets were converted into image datasets. The process commonly employed to convert one-dimensional data into three-dimensional image data is known as "time-series to image transformation." The dataset is divided into training and testing using k-fold cross-validation. Using the proposed and existing deep learning models, we have performed a binary and multi-class classification on all the IDS datasets CICIDS-2017, 2018 and UNSW-NB15. Table 2 presents the simulation parameters.

Table 2: Parameters used for simulation

Parameters	Details
CNN Model	Transfer Learning and Light-weight CNN (mobile-V3) with SVM
No Training Layers	100-250
Epochs	50-100
Optimizer used	Stochastic Gradient Descent (SGD) Optimizer
Model learning rate	0.001
Loss function	Categorical Cross Entropy (CCE) function
Activation function	SoftMax, ReLu
Batch size	256
Hidden Layer Architecture	(256,128,64)

4.1 Experimental results for CICIDS-2017

This dataset replicates the real-world data in PCAPs by including benign and the most recent examples of common attacks. It additionally contains the findings of an analysis of the network traffic performed with CIC_Flow_Meter complete with labelled flows organized according to the protocols, date and time stamp, origin and destination IP addresses, the source with destination port numbers, and attack. Figure 8 presents the visual of the attack class and normal class.



Journal Pre-proof

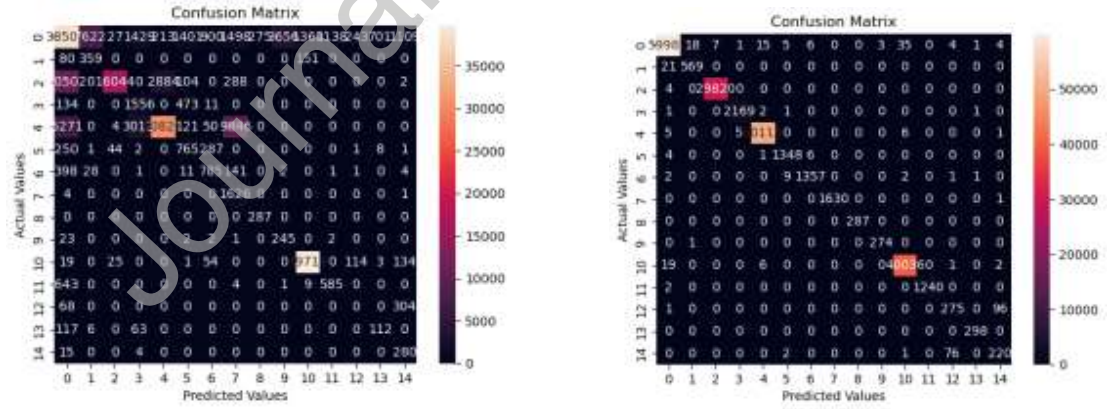
Figure 8: Visualization of Attack Class for CICIDS-2017

Table 3 presents the attack class type and count for the CICIDS-2017 dataset.

Table 3: Details of the CICIDS-2017 dataset

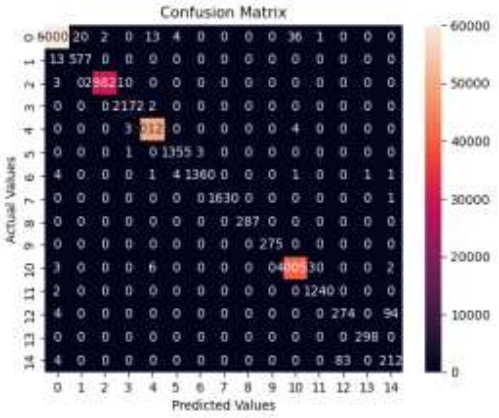
Attack Type	**Count**
BENIGN	68,2092
DoS Hulk	69,066
Ports can	47,841
DDoS	38,346
DoS Golden Eye	3,041
FTP-Patator	2,359
SSH-Patator	1,786
DoS slow_loris	1,764
DoS Slow_http_test	1,649
Bot	5,80
Web Attack and Brute Force	4,65
Web Attack and XSS	2,03
Infiltration	21
Web Attack and SQL Injection	8
Heart bleed	2
Total	**84,9223**

We have measured the Confusion matrix results for all the methods, i.e., existing and proposed on the given IDS dataset. Figure 9 presents a Confusion Matrix (a) for VGG-16 and (b) for VGG-19, (c) Efficient-Net and (d) Inception-Net and (e) proposed model. Similarly, Figure 10 shows an accuracy and loss curve, and Figure 11 shows the ROC curve for the CIC-IDS 2017 dataset for the proposed model.

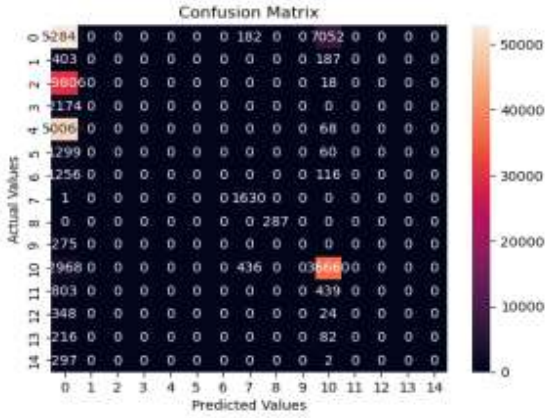


(a) VGG-16 (b) VGG-19

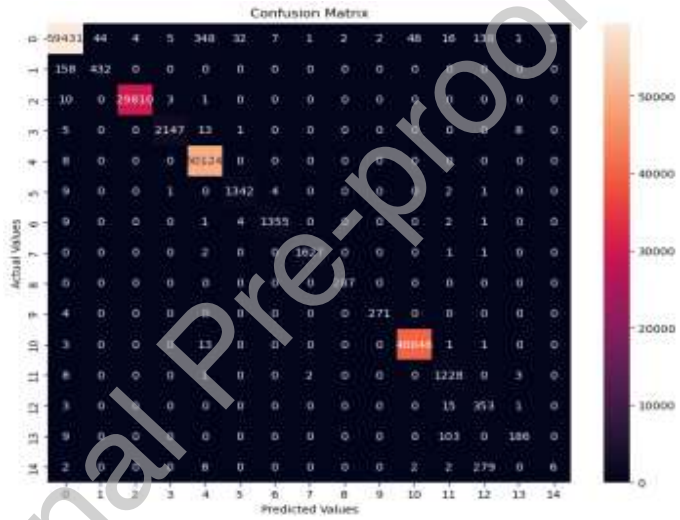
Journal Pre-proof



(C) Efficient-Net

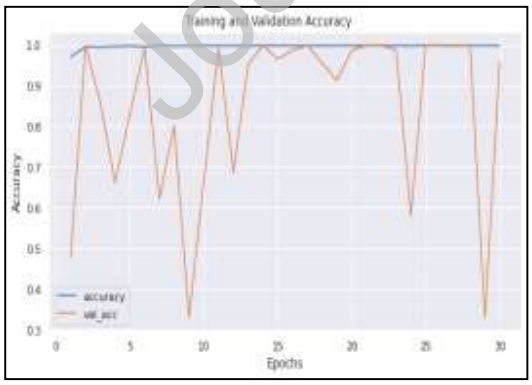


(d) Inception-Net

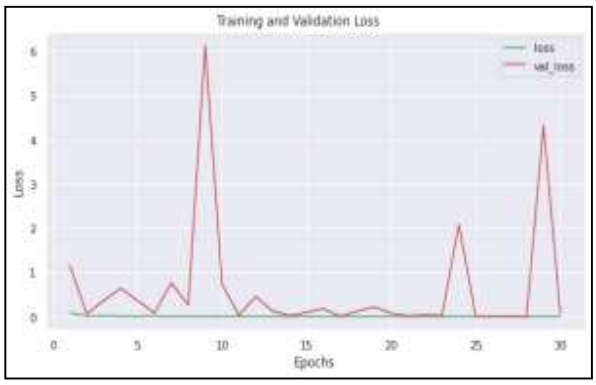


(e) Proposed model

Figure 9: Confusion Matrix of existing and proposed model for the CICIDS-2017 dataset



(a)



(b)

Figure 10: Accuracy and Loss Curve (Binary Classification) for CIC-IDS 2017 dataset for the proposed model

Journal Pre-proof

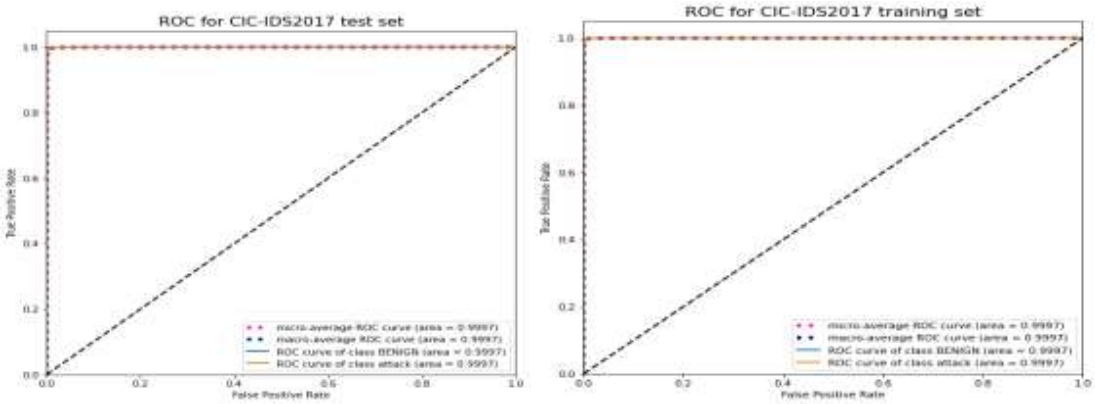


Figure 11: ROC curve (Binary Classification) for CIC-IDS 2017 dataset for the proposed model

Table 4 presents experimental results comparison on CICIDS-2017 for existing and proposed methods. VGG-16 method achieves a recall of 91.02%, precision 93.47%, F1-Score 93.28%, MSE 0.0153, RMSE 0.0166 and MAE 0.0165. VGG-19 method achieves Recall 95.34%, Precision 96.97% and F1-Score 95.38%, MSE 0.0166, RMSE 0.0177and MAE 0.0162. Efficient-Net method achieves Recall 94.07%, Precision 96.91% and F1-Score 96.21%, MSE 0.0171, RMSE 0.0178. and MAE 0.0170.

Table 4**:** Experimental results comparison on CICIDS-2017 for Multi-class classification

Model	Recall	Precision	F1-Score	MSE	RMSE	MAE
VGG-16	91.02%	93.47%	93.28%	0.0153	0.0166	0.0165
VGG-19	95.34%	96.97%	95.38%	0.0166	0.0177	0.0162
Efficient-Net	94.07%	96.91%	96.21%	0.0171	0.0178	0.0170
Inception-Net	96.55%	96.79%	97.35%	0.0181	0.0178	0.0181
Proposed Method	98.72%	98.91%	99.09%	0.0140	0.0137	0.0139

The inception-net method achieves Recall 96.55%, Precision 96.79% and F1-Score 97.35% MSE 0.0181, RMSE 0.0178, and MAE 0.0181. The proposed method achieves Recall 98.72%, Precision 98.91% and F1-Score 99.09%, MSE 0.0140, RMSE 0.0137 and MAE 0.0139.

Table 5: Accuracy results comparison for CICIDS-2017 for Multi-class classification

Attack Class	VGG-16	VGG-19	Efficient-Net	Inception-Net	Proposed Hybrid model
Web_Attack	89.78	90.12	86.35	92.24	98.98
DOS	90.23	91.45	85.6	91.65	99.01
Infiltration	88.97	89.65	88.69	92.33	98.32
DDOS	90.78	92.35	90.36	90.78	98.74
Port_Scan	91.45	93.45	91.65	92.35	98.17

We have calculated various performance measuring parameters for existing and proposed methods. Table 5 presents the accuracy results compared to the CICIDS-2017 dataset for existing and proposed methods for different classes. For class 'Web_Attack', the proposed method achieves 98.98% accuracy, for 'DOS' 99.01%', for Infiltration' 98.32%', for 'DDOS' 98.74% and for 'Port_Scan' 98.17% accuracy.

Journal Pre-proof

4.2 Experimental Results CIC-IDS 2018

The University of New Brunswick developed this dataset, initially intending to research DDoS details. The dataset was derived from log files of the institution's servers and revealed several different DoS attacks across the period in which that information was accessible to everyone. The dataset contains Benign: 38, 0943 and malicious: 38, 0943. We have split the dataset in training and testing using k-fold cross-validation. The training set contains Benign: 26, 6633 and Malicious: 26, 6687; the Test set contains Benign: 11, 4310 and Malicious: 11, 4256 elements. Figure 12 presents the Binary class classification of the CICIDS-2018 dataset. Figure 13 shows the Confusion Matrix results for (Binary Class-Classification) for the CICIDS-2018 dataset.

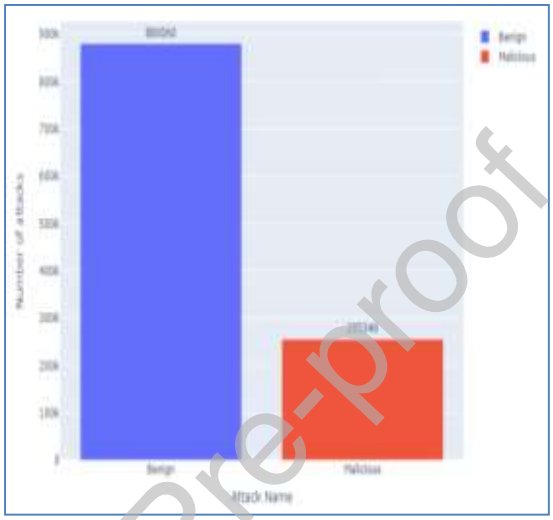
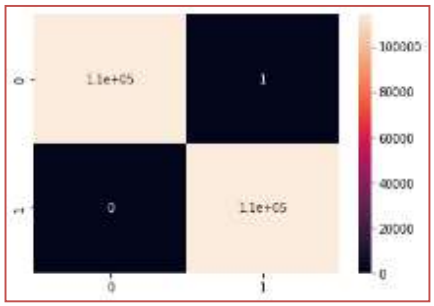
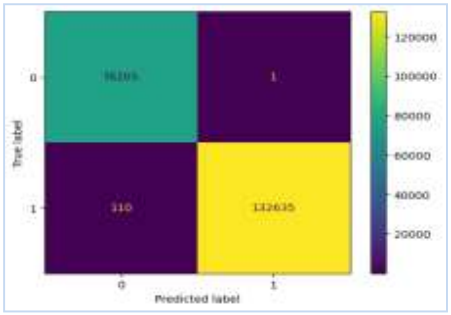


Figure 12: Binary class classification (Attack type) of the CICIDS-2018 dataset

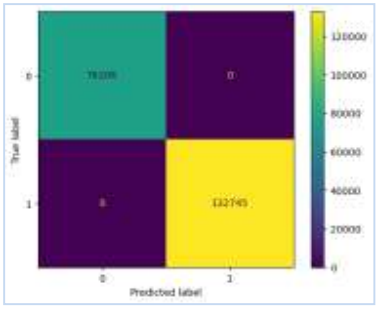
(a) VGG-16



(b) VGG-19

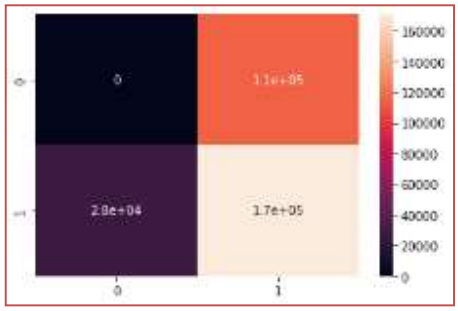


(c)Efficient-Net



(d) Inception-Net

Journal Pre-proof



(e) Proposed Method

Figure 13: Confusion Matrix (Binary Class-Classification) for CICIDS-2018 dataset

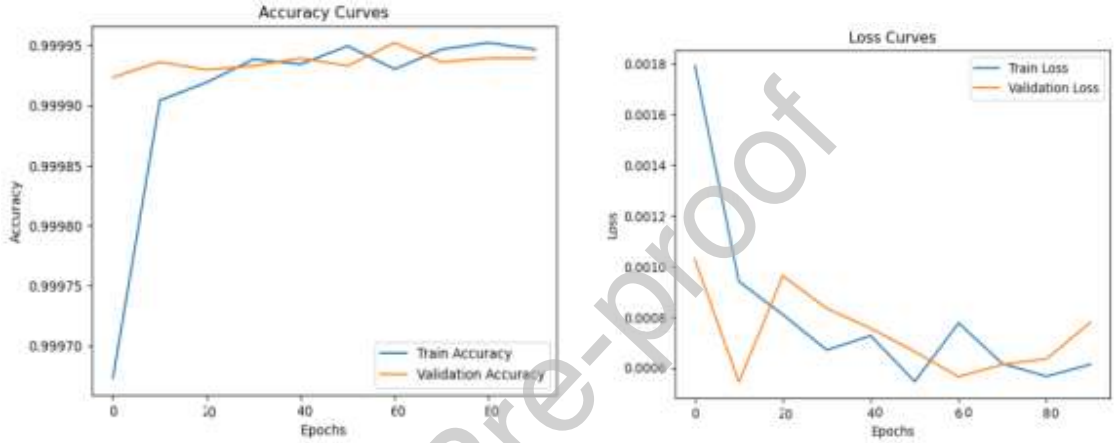


Figure 14: Accuracy and Loss curve for CIC-IDS 2018 dataset for the proposed model for Binary class

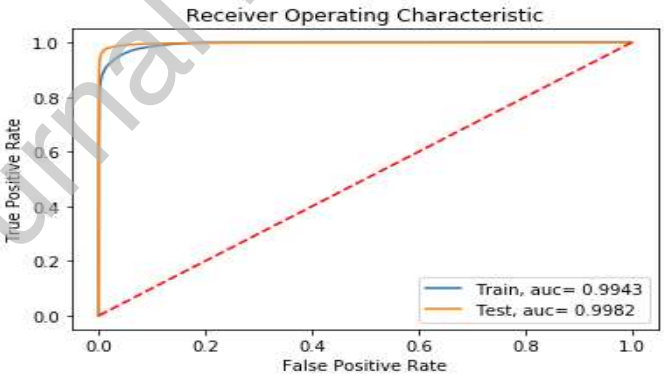


Figure 15: ROC curve (Binary class) for CIC-IDS 2018 dataset for the proposed model

Figure 14 shows the accuracy and loss curve, and Figure 15 shows the ROC curve for the binary class) for the CIC-IDS 2018 dataset for the proposed model.

Table 6: Experimental results comparison for Binary-class classification CICIDS-2018

Model	Recall	Precision	F1-Score	MSE	RMSE	MAE
VGG-16	92.32%	94.07%	92.08%	0.0145	0.0174	0.0155
VGG-19	96.74%	96.07%	94.08%	0.0174	0.0165	0.0164
Efficient-Net	96.87%	95.51%	97.01%	0.0168	0.0176	0.0176

Journal Pre-proof

Journal Pre-proof

Inception-Net	97.05%	95.09%	96.05%	0.0171	0.0166	0.0187
Proposed	99.32%	99.01%	98.99%	0.0141	0.0143	0.0140

Table 6 shows an experimental result comparison for the Binary-class classification CICIDS-2018 dataset. The proposed model achieves 99.01% precision, 99.32% Recall, 98.99 % F1-score, 0.0141 MSE, 0.0143 RMSE and 0.0140 MAE, which is better as compared to existing methods, i.e., VGG-16, VGG-19, Efficient-Net, Inception-Net and Proposed Method.

Table 7: Accuracy results comparison for Multi-class classification CICIDS-2018

Attack Class	VGG-16	VGG-19	Efficient-Net	Inception-Net	Proposed Hybrid model
Web_Attack	81.56	88.24	80.13	88.54	99.13
DOS	79.56	87.32	79.45	90.36	98.21
Infiltration	78.92	85.36	81.78	89.78	99.12
DDOS	80.36	89.55	88.69	89.45	97.36

Similarly, Table 7 shows the accuracy results from the comparison for Multi-class classification CICIDS-2018. The proposed method achieves an accuracy of 99.13%, Web_Attack 98.21%, DOS 99.12%, and Infiltration and DDOS 97.36%.

4.3 UNSW-NB15

The IXIA Perfect Storm, an instrument in the Cyber Range Laboratory at UNSW Canberra, Australia, generates the raw packets from the network comprising the UNSW-NB 15 dataset. This was done to generate a hybrid representation of actual modern routines and artificial modern attack behavioural patterns. The dataset contains 257,673 instances, of which 82,332 were used for training and 17,5341 for testing. Figure 16 presents the Training and testing dataset count for the Binary Classification of UNSW-NB15, and Figure 17 shows the Correlation Matrix of UNSW-NB15. Figure 18 shows a Confusion Matrix of (Binary Class-Classification) for UNSW-NB15.

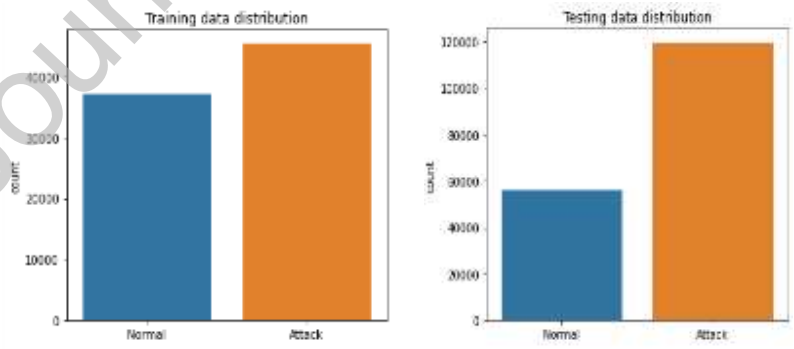


Figure 16: Training and testing dataset count for Binary Classification of UNSW-NB15

Journal Pre-proof

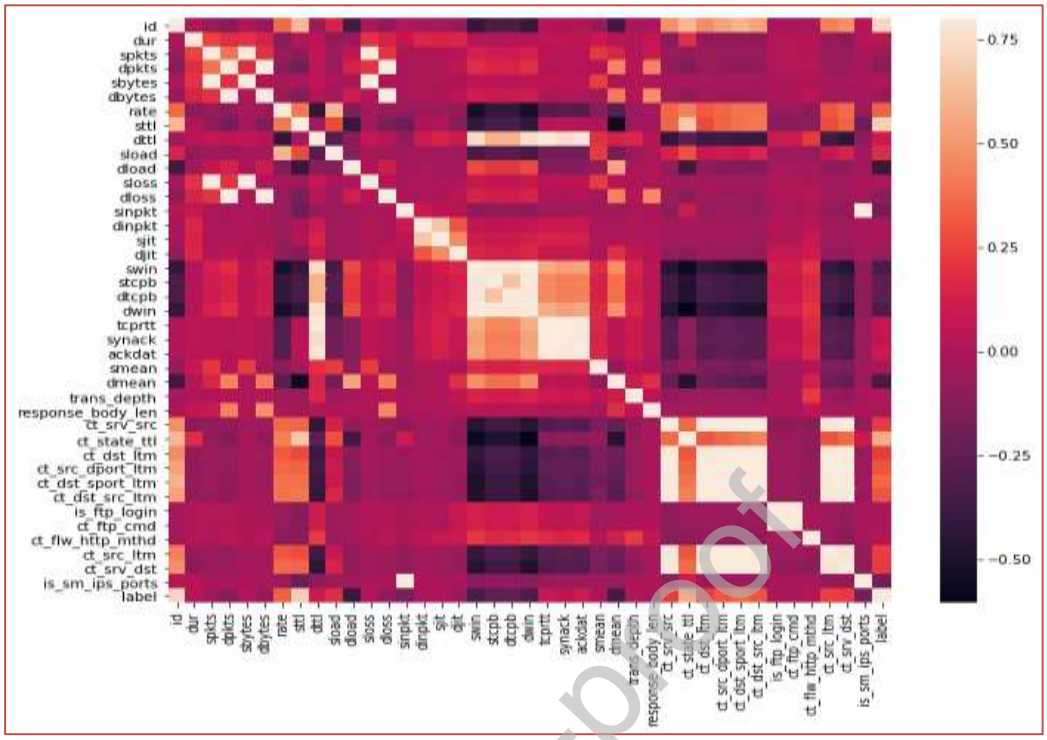
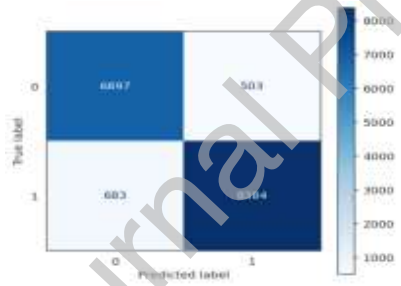
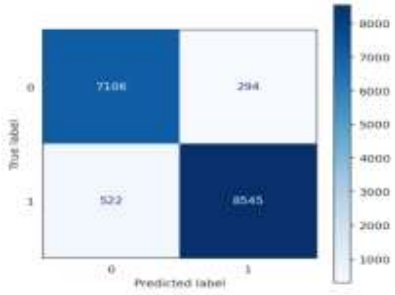


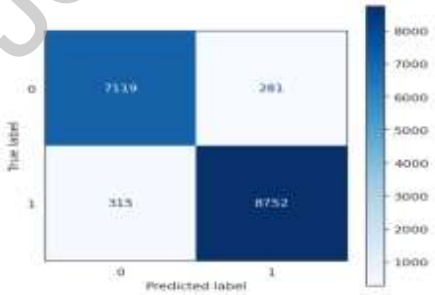
Figure 17: Correlation Matrix of UNSW-NB15



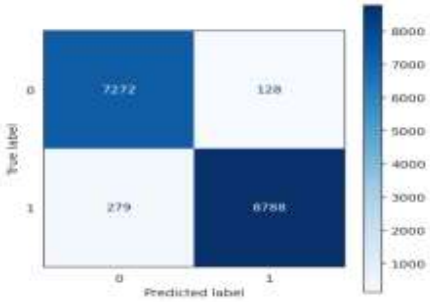
(a) VGG-16



(b) VGG-19

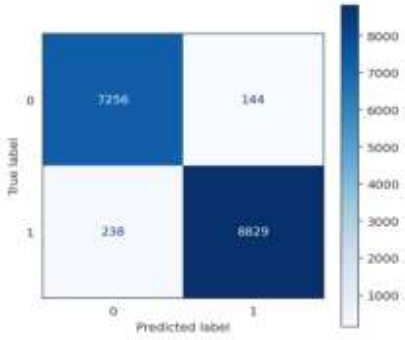


(c) Efficient-Net



(d) Inception-Net

Journal Pre-proof



(e) Proposed Method

Figure 18: Confusion Matrix of (Binary Class-Classification) for UNSW-NB15

Table 8: Experimental results comparison UNSW-NB15 for binary class classification

Model	Accuracy	Recall	Precision	F1-Score	MSE	RMSE	MAE
VGG-16	91.81%	91.98%	93.73%	93.18%	0.0151	0.0164	0.0145
VGG-19	95.79%	95.98%	97.78%	95.68%	0.0166	0.0154	0.0154
Efficient-Net	96.78%	96.73%	96.75%	96.33%	0.0164	0.0166	0.0166
Inception-Net	96.87%	96.35%	96.76%	96.75%	0.0164	0.0156	0.0177
Proposed	99.89%	98.98%	98.29%	98.79%	0.0130	0.0131	0.0130

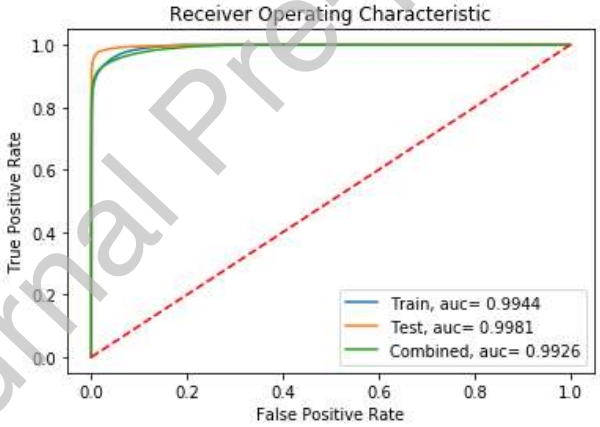


Figure 19: ROC curve to Binary-Class for UNSW-NB15 dataset for the proposed model

Table 8 compares experimental results for the (binary class classification) UNSW-NB15 dataset. The proposed model achieves an accuracy of 99.89%, Recall 98.98%, Precision 98.29%, F1-Score 98.79%, MSE 0.0130, RMSE 0.0131, and MAE 0.0130.

Journal Pre-proof

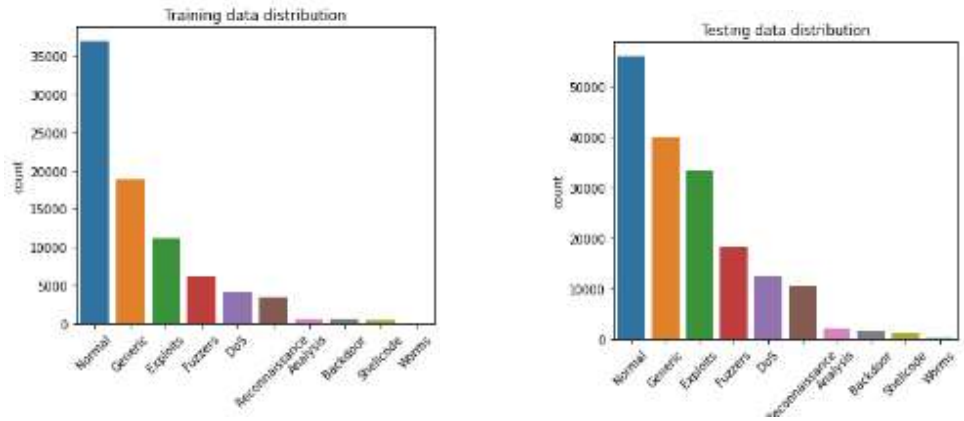


Figure 20: Training and testing dataset count for Multi-class Classification of UNSW-NB15

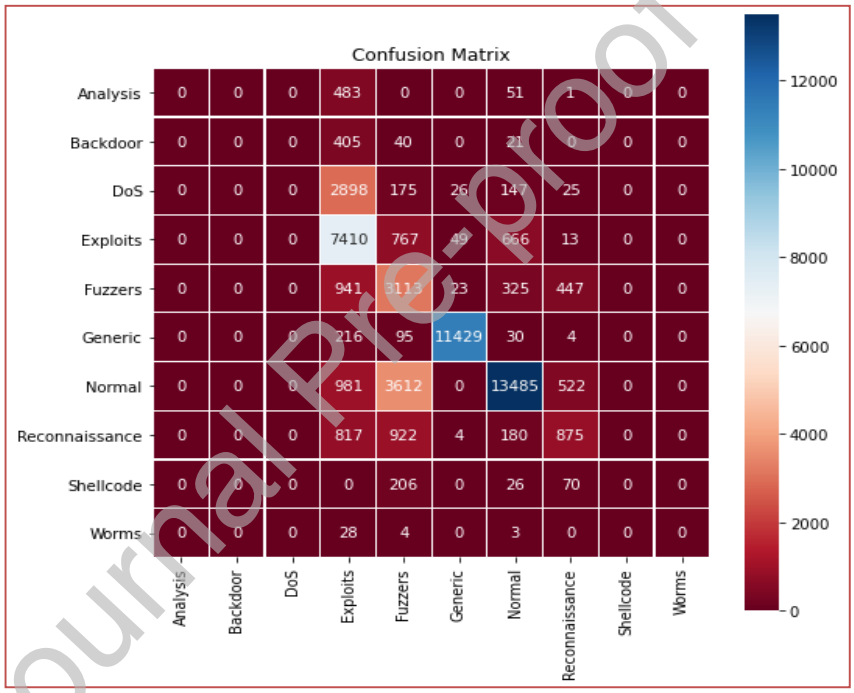


Figure 21: Confusion Matrix for UNSW-NB15 dataset of the proposed model for Multi-class

Journal Pre-proof

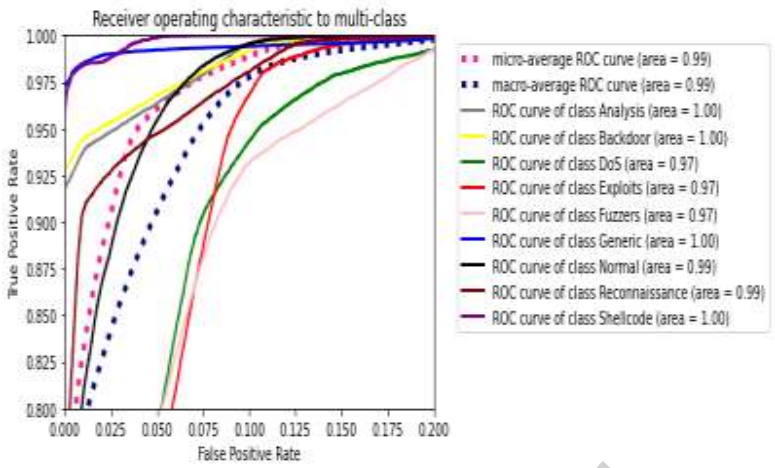


Figure 22: ROC curve to Multi-Class for UNSW-NB15 dataset for the proposed model

Figure 20 shows the training and testing dataset count for the Multi-class Classification of UNSW-NB15, Figure 21 shows a Confusion Matrix for the UNSW-NB15 dataset of the proposed model for Multi-class, and Figure 22 shows the ROC curve to Multi-Class for the UNSW-NB15 dataset for the proposed model. The proposed model achieves better results for all three IDS datasets, i.e., UNSW-NB15, CICIDS-2017, 2018, in terms of better Accuracy, Recall, Precision, F1-Score, MSE, RMSE and MAE as compared to existing models, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net for binary and multi-class classifications.

4.4 Results and Discussion

The hybrid model that combines an improved light-weight CNN configuration (MobileNetV3), transfer learning (TL), and SVM to detect intrusion in 5G wireless communication networks reveals considerable promise. The model demonstrates improved accuracy in detecting intrusions and a reduction in false positives due to applying MobileNetV3's effective feature identification and extraction abilities and transforming it to 5G-specific intrusion sequences by performing TL. The proposed hybrid model and existing models, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net, are implemented and compared on three benchmarks IDS datasets, i.e., CICIDS-2017, 2018 and UNSW-NB15.

The simulation results were calculated for the CICIDS-2017 dataset in the first experiment. Figure 9 presents a Confusion Matrix (a) for VGG-16 and (b) for VGG-19, (c) Efficient-Net and (d) Inception-Net and (e) proposed model and Figure 10 shows an accuracy and loss curve, and Figure 11 shows the ROC curve for CIC-IDS 2017 dataset for the proposed model. Table 4 presents experimental results comparison on CICIDS-2017 for existing and proposed methods. VGG-16 method achieves a recall of 91.02%, precision 93.47%, F1-Score 93.28%, MSE 0.0153, RMSE 0.0166 and MAE 0.0165. VGG-19 method achieves Recall 95.34%, Precision 96.97% and F1-Score 95.38%, MSE 0.0166, RMSE 0.0177and MAE 0.0162. Efficient-Net method achieves Recall 94.07%, Precision 96.91% and F1-Score 96.21%, MSE 0.0171, RMSE 0.0178, and MAE 0.0170. We have calculated various performance measuring parameters for existing and proposed methods. Table 5 presents the accuracy results compared to the CICIDS-2017 dataset for existing and proposed methods for different classes. For class

Journal Pre-proof

Journal Pre-proof

'Web_Attack', the proposed method achieves 98.98% accuracy, for 'DOS' 99.01%', for Infiltration' 98.32%', for 'DDOS' 98.74% and for 'Port_Scan' 98.17% accuracy.

The second experiment was conducted on the CIC-IDS 2018 dataset. Table 6 shows an experimental result comparison for the Binary-class classification CICIDS-2018 dataset. The proposed model achieves 99.01% precision, 99.32% Recall, 98.99 % F1-score, 0.0141 MSE, 0.0143 RMSE and 0.0140 MAE, which is better as compared to existing methods, i.e., VGG-16, VGG-19, Efficient-Net, Inception-Net and Proposed Method. Similarly, Table 7 shows the accuracy results from the comparison for Multi-class classification CICIDS-2018. The proposed method achieves an accuracy of 99.13%, Web_Attack 98.21%, DOS 99.12%, and Infiltration and DDOS 97.36%.

The third experiment was conducted on UNSW-NB15. Table 8 compares experimental results for the (binary class classification) UNSW-NB15 dataset. The proposed model achieves an accuracy of 99.89%, Recall 98.98%, Precision 98.29%, F1-Score 98.79%, MSE 0.0130, RMSE 0.0131, and MAE 0.0130. Figure 20 shows the training and testing dataset count for the Multi-class Classification of UNSW-NB15, Figure 21 shows a Confusion Matrix for the UNSW-NB15 dataset of the proposed model for Multi-class, and Figure 22 shows the ROC curve to Multi-Class for the UNSW-NB15 dataset for the proposed model. The proposed model achieves better results for all three IDS datasets, i.e., UNSW-NB15, CICIDS-2017, 2018, in terms of better Accuracy, Recall, Precision, F1-Score, MSE, RMSE and MAE as compared to existing models, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net for binary and multi-class classifications.

The proposed model performed well over existing VGG-16, VGG-19, Efficient-Net and Inception-Net models for several reasons.

- **Efficiency and Scalability of MobileNetV3:** The MobileNetV3 architecture is specifically engineered to prioritize computational efficiency and light-weight characteristics, rendering it highly suitable for environments with limited resources. In the realm of 5G communication and intrusion detection, the utilization of MobileNetV3's efficiency can prove advantageous due to its ability to facilitate real-time processing and scalability, which are crucial factors in this context. It necessitates a reduced amount of computational resources while maintaining the ability to capture pertinent features accurately.
- **Transfer learning**: It refers to the process by which a model can utilize the knowledge it has acquired from one dataset, such as ImageNet, and effectively apply it to the intrusion detection domain. Transferring knowledge can greatly enhance performance, particularly in cases where the target domain, such as intrusion detection, possesses a smaller dataset than the source domain, like ImageNet. Transport Layer facilitates the model's adaptation to the distinctive attributes of network traffic data, thereby enhancing its proficiency in detecting intrusions.
- **Adaptation to Intrusion Patterns:** The hybrid architecture has been specifically optimized for intrusion detection, allowing for better adaptation to intrusion patterns. The proposed design has the

Journal Pre-proof

potential to effectively capture specific features and patterns that are highly pertinent to the various types of attacks and anomalies observed in network traffic data. Consequently, it is expected to perform better than more generic convolutional neural network architectures such as VGG-16 or VGG-19.

- **Reduced Risk of Overfitting:** Light-weight architectures such as MobileNetV3 can mitigate the overfitting risk, particularly in limited datasets. The issue of overfitting may arise in the context of intrusion detection, particularly when dealing with imbalanced and noisy data. MobileNetV3 exhibits the potential for enhanced robustness in such scenarios by effectively extracting pertinent features and exhibiting reduced complexity.
- **Efficient Hyperparameter Tuning:** The proposed model may have undergone significant hyperparameter tuning, which encompasses the selection of kernel functions, SVM factors, and fusion techniques. The meticulous refinement of these aspects can substantially influence the model's performance and contribute to its superiority compared to other models. The IDs datasets CICIDS-2017, CICIDS-2018, and UNSW-NB15 exhibit characteristics compatible with the strengths of MobileNetV3-SVM. The model's architecture and transfer learning approach may have been designed to leverage the dataset's characteristics effectively.
- **Advancements in Neural Network Architectures:** The field of neural network architectures has experienced significant progress and refinement, owing to the continuous advancements in the design of neural network structures and the utilization of transfer learning methodologies. The MobileNetV3 architecture, being a more contemporary design, derives advantages from these technological advancements and potentially exhibits superior performance compared to earlier models.

Journal Pre-proof

4.4.1 Application Scenarios

The hybrid model has many practical applications, which employ transfer learning (TL) and improved light-weight CNN architecture (MobileNetV3-SVM) for identifying intrusions in 5G networks for communication. As mentioned in earlier scenarios, the application underscores the adaptability and significance of the MobileNetV3-SVM hybrid model in intrusion detection within 5G communication networks. The secure and efficient operation of 5G technology is crucial for safeguarding various industries and critical functions. There exist numerous possible application cases for this framework are as follows.

- **5G Network Security:** The primary objective of 5G network security is to augment the security measures implemented in 5G communication networks. The deployment of the model within the network infrastructure enables real-time monitoring of traffic, detection of intrusions, and prompt

Journal Pre-proof

response to security threats. The measures mentioned earlier are implemented to preserve the integrity, availability, and confidentiality of 5G network services.

- **Smart Cities:** The establishment of smart cities entails the utilization of 5G networks to enable an extensive range of facilities and infrastructure development. The utilization of this model has the potential to augment the security of critical urban functions, encompassing transportation networks, security policies, energy administration, and medical care. The system can detect and mitigate possible hazards and weaknesses present in these interconnected systems.
- **IoT Device Security:** Using 5G networks plays a crucial role in protecting Internet of Things (IoT) devices and applications from potential cyber threats within the realm of IoT device security. The system can detect and address occurrences of unauthorized access, violations of data security, and deliberate attacks aimed at Internet of Things (IoT) devices and networks.
- **Industrial IoT (IIoT):** The term "industrial adoption of 5G technology" pertains to the application of fifth-generation wireless technology by different industries to protect manufacturing operations, distribution networks, and vital infrastructure from possible cyber-attacks. The system possesses the capability to identify anomalies that possess the capacity to impede operational procedures or jeopardize safety protocols.
- **Financial Services:** The financial services sector predominantly employs 5G networks for trading with high frequencies and low-latency financial transactions. The application of this model can enhance the security protocols employed in financial systems, proficiently detect occurrences of deceptive conduct, and strengthen safeguards against cyber risks that concentrate on financial establishments.
- **Critical Infrastructure Protection:** The model can protect critical infrastructure, including power grids, water treatment plants, and transportation hubs, which heavily depend on 5G connectivity. The system possesses the capability to identify and counteract cyber threats that have the potential to disrupt these vital services.
- **Telemedicine and Healthcare:** The importance of protecting individual patient information and communication is of the utmost significance in the growing adoption of telemedicine services and distant healthcare tracking enabled by 5G networks. The utilization of the model has the potential to augment the privacy of medical facilities through the mitigation of data breach risks and the assurance of clinical data confidentiality.
- **Autonomous Vehicles:** The significance of 5G communications in autonomous public transportation resides in its facilitation of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) conversation. The application of this model can significantly bolster the security of these

Journal Pre-proof

communications, thereby reducing the likelihood of possible attacks on self-driving automobiles that could lead to incidents.

- **Edge Computing Security:** The topic of edge computing security is of great significance due to the increasing prevalence of edge computing in 5G networks. This model allows for deployment at the network edge, enabling the monitoring and safeguarding data processing at the edge devices. The primary objective is to ensure the preservation of data confidentiality and integrity.
- **Cloud Security:** Within cloud computing environments that employ 5G networks for connectivity, this model can be an integral component of a comprehensive security approach. Its primary functions encompass monitoring network traffic, identifying intrusions, and safeguarding cloud-based resources and data.
- **Compliance and Regulatory Requirements:** Using the model can aid organizations in adhering to regulatory requirements, specifically data protection laws, by guaranteeing the security and privacy of data transmitted through 5G networks.
- **Military and Defense:** In the realm of military applications, using the model becomes imperative in safeguarding military networks and communication systems against cyber threats and espionage due to the paramount importance of secure and dependable communication.

5 Conclusion and future works

5G networks mainly support most commercial applications running in the real world. Such applications offer sufficient potential to serve as the cornerstone of a constantly connected community. Despite this, there are still issues with the architecture, the time of release, and deployment, which are important to researchers working on all 5G networks. One of the most critical of these research issues is promptly detecting unauthorized access instances, particularly in networks businesses use. As a result, the most recent findings from research on this extremely significant subject are presented here in this work. In addition, this article describes an accurate intrusion detection and classification model using a light-weight CNN deep learning.

A light-weight CNN model with a transfer learning method is a promising strategy for building effective and precise intrusion detection algorithms for IoT and 5G wireless networks. The proposed hybrid method incorporates the benefits of light-weight structures, transfer learning, and job-specific fine-tuning to develop frameworks capable of handling the obstacles of resource limitations while effectively identifying intrusions in unpredictable network conditions. Finally, the outcome proves that the proposed security model for IoT and 5G networks more precisely detects intrusion in dynamic situations. Its light-weight architecture and capacity to learn from multiple sources of information make the model an intriguing approach to improving IoT and 5G network security in the context of changing cyber risks. The proposed model achieves better results for all three IDS datasets, i.e., UNSW-NB15, CICIDS-2017, 2018, in terms of better Accuracy, Recall, Precision, F1-Score, MSE, RMSE and MAE as compared to existing models, i.e., VGG-16, VGG-19, Efficient-Net and Inception-Net for binary and multi-class classifications. It shows the strength of the proposed model. In future work,

Journal Pre-proof

we will work on reducing the time complexity of the proposed model and implementing the model in a real-time environment.

Conflict of Interests: The authors declared that they have no conflict of interest.
Funding: No funding was received for this research.
Availability of Data and Materials: The dataset is available with the corresponding author and available based on individual request.
Ethics Approval and Consent to Participate: Not applicable.
Consent for Publication: The authors are willing to permit the Journal to publish the article.
Acknowledgements: None
Authors' Contributions Umesh Kumar Lilhore: Conceptualization, Review & Editing, Writing Original Draft. Sarita Simaiya: Conceptualization, Data Curation, Formal analysis, Software, Methodology, Revised manuscript, Visualization, Writing - Review & Editing, Writing Original Draft. Surjeet Dalal: Investigation, Review & Editing, Writing Original Draft. Surjeet Dalal: Methodology, Writing Original Draft, Writing - Review & Editing.

References

1. Jeon SE, Lee SJ, Lee IG. Machine Learning-Based Efficient Discovery of Software Vulnerability for Internet of Things. Intelligent Automation & Soft Computing. 2023 Aug 1; 37(2).
2. Sharma, H., & Kumar, N. (2023). Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey. *Physical Communication*, 102002.
3. Lv, Z., Chen, D., Cao, B., Song, H., & Lv, H. (2023). Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins. *IEEE Transactions on Computers*.
4. Cui, J., Sun, H., Zhong, H., Zhang, J., Wei, L., Bolodurina, I., & He, D. (2023). Collaborative Intrusion Detection System for SDVN: A Fairness Federated Deep Learning Approach. *IEEE Transactions on Parallel and Distributed Systems*.
5. Park, C., Park, K., Song, J., & Kim, J. (2023, June). Distributed Learning-Based Intrusion Detection in 5G and Beyond Networks. In *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 490-495). IEEE.
6. Chakraborty, S., Pandey, S. K., Maity, S., & Dey, L. (2023). Detection and Classification of Novel Attacks and Anomaly in IoT Network using Rule based Deep Learning Model. *arXiv preprint arXiv:2308.00005*.
7. Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly Detection in 6G Networks Using Machine Learning Methods. *Electronics*, *12*(15), 3300.
8. Jadav, N. K., Kakkar, R., Mankodiya, H., Gupta, R., Tanwar, S., Agrawal, S., & Sharma, R. (2023). GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G. *Digital Communications and Networks*, *9*(2), 422-435.
9. Sood, K., Nosouhi, M. R., Nguyen, D. D. N., Jiang, F., Chowdhury, M., & Doss, R. (2023). Intrusion detection scheme with dimensionality reduction in next generation networks. *IEEE Transactions on Information Forensics and Security*, *18*, 965-979.
10. Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H., & Al-Absi, M. A. (2023). Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet of Things Journal*.
11. Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., ... & Marina, V. (2023). Deep learning-based malicious smart contract and intrusion detection system for IoT environment. *Mathematics*, *11*(2), 418.
12. Chauhdary, S. H., Alkatheiri, M. S., Alqarni, M. A., & Saleem, S. (2023). An efficient evolutionary deep learning-based attack prediction in supply chain management systems. *Computers and Electrical Engineering*, *109*, 108768.

Journal Pre-proof

13. Uszko, K., Kasprzyk, M., Natkaniec, M., & Chołda, P. (2023). Rule-Based System with Machine Learning Support for Detecting Anomalies in 5G WLANs. *Electronics*, *12*(11), 2355.

14. Zhang, H., Xie, R., Li, K., Huang, W., Yang, C., & Liu, J. (2023, July). Anomaly Detection Based on Deep Learning: Insights and Opportunities. In *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 30-36). IEEE.

15. Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion detection system on IoT with 5G network using deep learning. *Wireless Communications and Mobile Computing*, *2022*, 1-13.

16. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) dataset, Acess on 5th Jan 2023, available at https://registry.opendata.aws/cse-cic-ids2018/

17. Rajasoundaran, S., Prabu, A. V., Routray, S., Malla, P. P., Kumar, G. S., Mukherjee, A., & Qi, Y. (2022). Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks. *Computer Communications*, *187*, 71-82.

18. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.

19. Jagannath, J., Ramezanpour, K., & Jagannath, A. (2022, May). Digital twin virtualization with machine learning for IoT and beyond 5G networks: Research directions for security and optimal control. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning* (pp. 81-86).

20. Sharma, H., & Kumar, N. (2023). Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey. *Physical Communication*, 102002.

21. Intrusion Detection Evaluation Dataset (CIC-IDS2017), access on 3rd Jan 2023, available at https://www.unb.ca/cic/datasets/ids-2017.html

22. Intrusion Detection Evaluation Dataset (CIC-IDS2018), access on 5th Jan 2023, available at https://www.unb.ca/cic/datasets/ids-2018.html.

23. Intrusion Detection Evaluation Dataset (UNSW-NB15), access on 5th Jan 2023, available at https://www.kaggle.com/datasets/dhoogla/unswnb15

24. Wang, X., Wang, Y., Javaheri, Z., Almutairi, L., Moghadamnejad, N., & Younes, O. S. (2023). Federated deep learning for anomaly detection in the internet of things. *Computers and Electrical Engineering*, *108*, 108651.

25. Ahmed, I., Anisetti, M., Ahmad, A., & Jeon, G. (2022). A Multi-layer Deep Learning Approach for Malware Classification in 5G-Enabled IIoT. *IEEE Transactions on Industrial Informatics*, *19*(2), 1495-1503.

26. Abbas, G., Mehmood, A., Carsten, M., Epiphaniou, G., & Lloret, J. (2022). Safety, Security and Privacy in Machine Learning Based Internet of Things. *Journal of Sensor and Actuator Networks*, *11*(3), 38.

27. Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors*, *22*(2), 528.

28. Jeon, S. E., Lee, S. J., & Lee, I. G. (2023). Machine Learning-Based Efficient Discovery of Software Vulnerability for Internet of Things. *Intelligent Automation & Soft Computing*, *37*(2).

29. Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, *2*(04), 190-199.

30. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2020). Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics*, *9*(1), 173.

31. Venkatraman, S., & Surendiran, B. (2020). Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems. *Multimedia Tools and Applications*, *79*(5-6), 3993-4010.

32. Kumari, A., & Mehta, A. K. (2020, October). A hybrid intrusion detection system based on decision tree and support vector machine. In *2020 IEEE 5th International conference on computing communication and automation (ICCCA)* (pp. 396-400). IEEE.

Journal Pre-proof

Journal Pre-proof

33. Ramadan, R. A., & Yadav, K. (2020). A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516-0281.

34. Lv, L., Wang, W., Zhang, Z., & Liu, X. (2020). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. *Knowledge-based systems*, *195*, 105648.

Biography

Prof. (Dr.) Surjeet Dalal

Professor, Department of Computer Science and Engineering

Amity University Haryana, Gurugram-122403, India

E-mail: sdalal@ggn,amity.edu, profesurjeetdalal@gmail.com

Working as a Professor at Amity University, Dept. of CSE. He has gained more than 18+ years of teaching experience and 10 years of research experience. He is working as a Professor at Amity University, Dept. of CSE. He completed the PhD degree in 2017 and M Tech degree in CSE. He has published 40+ articles in reputed, peer-reviewed national and international Scopus journals and conferences.

Additionally, he has served as a keynote speaker and resource person for several workshops and webinars conducted in India. He has been an ACM and IEEE professional member. His research includes digital transformation technologies such as Artificial Intelligence (AI), Quantum Computing, Internet of Things (IoT), Blockchain, Edge and Serverless computing, Cloud-native computing and Digital Twins.

Google Scholar ID:
https://scholar.google.com/citations?user=owelGWAAAAAJ&hl=en

ORCID ID/Link: https://orcid.org/0000-0002-4325-9237

Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57190939535

Publons ID/Link: https://publons.com/researcher/3576607/surjeet-dalal/ LinkedIn Link: https://www.linkedin.com/in/prof-dr-surjeet-dalal-69694128/

Journal Pre-proof

Journal Pre-proof

Credit author statement

Umesh Kumar Lilhore: Conceptualization, Writing - Review & Editing, Writing Original Draft.

Sarita Simaiya: Conceptualization, Data Curation, Formal analysis, Software, Methodology, Revised manuscript, Visualization, Writing - Review & Editing, Writing Original Draft.

Surjeet Dalal: Methodology, Investigation, Writing - Review & Editing, Writing Original Draft.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Journal Pre-proof