Journal of Network and Information Security
13 (1) 2025, 01-17
www.publishingindia.com/jnis

Using Machine Learning to Detect Unusual Patterns and Behaviors in Network Security

Hameeda Abubakar Aminu[1] and Jesse Mazadu Ismaila[2*]
[1]Computer Science Department, Federal University Wukari, Nigeria.
Email: hameejal07@gmail.com
[2]Computer Science Department, Federal University Wukari, Nigeria.
Email: jesse@fuwukari.edu.ng
[*]Corresponding Author

Abstract: The development of the network anomaly detection model leveraged the computational robustness of the Anaconda programming environment. The concluding phase of this study, classification and performance evaluation, leverages features selected through the LDA algorithm to train machine learning classification models. Algorithms such as Random Forest and Support Vector Machine are employed, and the individual models undergo rigorous evaluation using metrics such as accuracy, precision, recall, and F1-score. This meticulous evaluation process ensures the reliability and efficacy of the models in discerning network intrusions. The Support Vector Machine (SVM) classification report for network anomaly detection using the CIC-DDoS2019 dataset indicates high performance across various evaluation metrics. With a precision of 0.9966 for class 0 and 0.9973 for class 1, the SVM demonstrates a strong ability to accurately classify instances of both normal and anomalous network traffic. Similarly, the recall scores of 0.9973 for class 0 and 0.9965 for class 1 indicate the model's effectiveness in identifying the majority of instances belonging to each class. The F1 scores, which consider both precision and recall, are also high for both classes, with values of 0.9970 for class 0 and 0.9969 for class 1. Moreover, the overall accuracy of the SVM model is reported as 0.9969, indicating its ability to correctly classify a large proportion of instances in the dataset. By delineating the research methodology into these phases, leveraging advanced computational tools and libraries, and reporting high-performance metrics for the SVM model, this study presents a comprehensive framework for developing an effective network anomaly detection system using machine learning algorithm.

Keywords: Anomaly, Detection, Intrusion, Network, Support vector machine.

I. Introduction

Background of the Study

The advent of Internet technology has ushered in an era of remarkable technological progress, yet alongside these advancements; it has also introduced new avenues for network intrusion and privacy breaches [1]. Consequently, anomaly detection has emerged as a critical endeavour across diverse fields, drawing upon centuries of research and development. Over time, a myriad of methodologies has been devised and deployed to address this challenge, spanning various domains and applications. At its essence, anomaly detection entails the identification of patterns within data that diverge from expected norms, as outlined by [2]. The significance of anomaly detection is

profound and far-reaching, given the inherent risks associated with undetected anomalies, which often carry pivotal and actionable insights. For instance, anomalies in computer network traffic may signify a cyber-attack stemming from a compromised system, while anomalies in credit card transaction data could indicate fraudulent activities such as theft.

Surveys conducted have revealed that firewalls, Deep Packet Inspection (DPI) systems and Intrusion Detection Systems (IDS) are the typical methods for anomaly detection, however, the cost to deploy these countermeasures and the complexity of the system have to be considered [3]. Hence, several researchers have applied the viabilities of Machine Learning (ML) algorithms to security in various types of network anomalies, from the traditional computer network to the IoT network [4]. However, the dataset employed for anomaly analysis is extensive, resulting in a notable decline in the efficiency of the machine learning algorithm. Authors have commonly resorted to feature selection methods to address the challenge of dataset dimensionality. A. Bemmert *et al.* [5] noted that feature selection involves reducing high-dimensional datasets to retain only the most relevant features for analysis.

The efficacy of machine learning (ML) techniques, coupled with a feature selection strategy, has been promising, leading to the proposal of employing Support Vector Machine (SVM) and Random Forest (RF) algorithms on the Canadian Institute for Cybersecurity - Distributed Denial of Service 2019 (CIC-DDoS2019) dataset sourced from the Mendeley machine learning repository. A factual reason is that upon examining the dataset, it became evident that its abundance of features could potentially hinder the efficiency of the models. Consequently, the study advocates for the implementation of the Linear Discriminant Algorithm (LDA) for feature selection. Thus, a significant contribution of this research lies in leveraging the LDA algorithm to select features before applying the SVM and RF algorithms for further feature selection.The rapid evolution of network technology has led to a proliferation of network services and applications, providing hackers with expanded avenues to compromise network security. Of particular concern is the paradigm shift in operational frameworks between next-generation networks and legacy systems, posing new challenges for anomaly detection methods [6]. To address these evolving threats and adapt to dynamic network environments, there is a pressing need for the advancement of anomaly detection techniques. Consequently, this study aims to explore the efficacy of Support Vector Machine (SVM) and Random Forest (RF) machine learning algorithms, augmented by feature selection using the linear discriminant algorithm, in mitigating emerging security threats within modern network infrastructures. The aim of this study is to develop a network anomaly detection system using machine learning algorithms. The objectives include:

- Perform feature selection using the LDA algorithm.
- Apply the viabilities of the SVM and RF algorithm for the detection of network anomaly.
- Evaluate the performance of the models using the accuracy, precision and recall metrics.

The significance of this study is multifaceted and crucial in the realm of cybersecurity. The escalating sophistication of cyber threats, poses an urgent demand for robust network anomaly detection systems to bolster defence mechanisms against potential breaches. By leveraging the SVM and RF machine learning algorithms and feature selection techniques, this study aims to elevate the accuracy and efficacy of anomaly detection processes. Such enhancements are pivotal in fortifying network security measures and preemptively identifying anomalous activities that may indicate malicious intent or cyber-attacks. Moreover, the outcomes of this research hold practical implications for various stakeholders, including network administrators, cybersecurity professionals, and organizations at large. Armed with insights gleaned from this study, these entities can make informed decisions and implement proactive measures to safeguard their networks, assets, and sensitive data from emerging cybersecurity threats. Thus, the significance of this study lies in its potential to contribute to the ongoing efforts to fortify cybersecurity defences and

mitigate the risks posed by network anomalies and cyber-attacks.

II. Literature Review

A. Theoretical Review

The rapid growth of computer networks has enabled them to function as a central information system in modern life. The increase in the size, services and applications, and infrastructure of computer networks such as the Internet of Things, has made them complex and heterogeneous. Thus, they confront various critical threats such as malicious activities, network intruders and cybercriminals. Identifying and preventing these detrimental cyber activities are a high priority these days [7]. Analyzing and monitoring network traffic to identify such malicious actions in large-scale networks are crucial tasks, and ideally should be carried out automatically with little supervision by network administrators [8]. Anomaly detection is a data analysis task where the goal is to detect patterns deviating greatly from normal data. It is suitable for automatically identifying illegal, malicious activities and other forms of network abuse from the normal behaviors of network systems. Anomalies pose a problem in various application areas, such as manufacturing, medical or communication systems. They often lead to a decrease in system performance and can cause instabilities and failure. Often, the cause of anomalies is unknown effects within complex systems. Therefore, the capability of understanding and detecting these underlying effects with the aid of data is the key to ensuring the desired outcome of complex technical systems [9].

B. Feature Selection

Feature selection is a technique that reduces dimensionality by retaining only relevant qualities and eliminating unnecessary and redundant ones [10]. Reducing the dimensionality of input can improve performance in two ways: it can improve generalization and classification accuracy but also slow learning and increase model complexity. Selecting the right characteristics can improve problem comprehension and reduce measurement costs. In some cases, feature selection can make a big difference. For example, only two characteristics out of 7129 can be employed to improve classification performance in microarray data processing. Reducing the dimensionality of problems while reducing related costs is the aim of feature selection in machine learning, and deep learning methodologies. Such applications include, for example, deriving information from photographs and interpreting expert differences in illness diagnosis. Filter, wrapper, and embedding approaches are some of the feature selection strategies [11].

C. Review of Related Works

Related works on anomaly detection are presented according to machine learning approaches and deep learning approaches thus:

i) Machine Learning Approaches

M. Nicolau, and J. McDermott [12] implemented a learning neural representation for network anomaly detection. Their paper proposed a latent representation model for improving network anomaly detection. Well-known anomaly detection algorithms often suffer from challenges posed by network data, such as high dimension and sparsity, and a lack of anomaly data for training, model selection, and hyperparameter tuning. Their approach was to introduce new regularizes to a classical autoencoder (AE) and a variational AE, which force normal data into a very tight area centered at the origin in the nonsaturating area of the bottleneck unit activations. These trained AEs on normal data will push normal points toward the origin, whereas anomalies, which differ from normal data, will be put far away from the normal region. The models were very different from common regularized AEs, sparse AEs, and contractive AEs, in which the regularized AEs tend to make their latent representation less sensitive to changes in the input data. The bottleneck feature space was now used as a new data representation. Several one-class learning algorithms were used for evaluating the proposed models. The experiments revealed that their models helped these classifiers to perform efficiently and consistently on high-

dimensional and sparse network datasets, even with relatively few training points. More importantly, the models can minimize the effect of model selection on these classifiers since their performance was insensitive to a wide range of hyperparameter settings.

D. Kwon *et al*. [13] performed an empirical study on network anomaly detection using convolutional neural networks. In their study, they empirically evaluated a set of deep learning models, including Fully Connected Network (FCN), Variational Auto Encoder (VAE), and Sequence to Sequence model with Long Short-Term Memory (Seq2Seq-LSTM), for network anomaly detection. In addition, they further evaluated Convolution Neural Networks (CNNs) for network anomaly detection in this study. They set up three simple CNN models with different internal depths (shallow CNN, moderate CNN, and deep CNN) to see the impact of the depth on the performance. They now evaluated the models using three different types of traffic datasets. Their experimental results show that deeper structures do not make any performance improvement. In addition, they observed that the evaluated CNN models occasionally outperform the VAE models, but do not work better than the other deep learning models based on FCN and Seq2Seq-LSTM.

B. J. Radford *et al.* [14] in their work "Network traffic anomaly detection using recurrent neural networks" showed that a recurrent neural network can learn a model to represent sequences of communications between computers on a network and can be used to identify outlier network traffic. Defending computer networks is a challenging problem and is typically addressed by manually identifying known malicious actor behaviour and then specifying rules to recognize such behaviour in network communications. However, these rule-based approaches often generalize poorly and identify only those patterns that are already known to researchers. An alternative approach that does not rely on known malicious behaviour patterns can potentially also detect previously unseen patterns. They tokenize and compress netflow into sequences of "words" that form "sentences" representative of a conversation between computers. These sentences were then used to generate a model that learns the semantic and syntactic grammar of the newly generated language. They use Long-Short-Term Memory (LSTM) cell Recurrent Neural Networks (RNN) to capture the complex relationships and nuances of this language. The language model was then used to predict the communications between two IPs and the prediction error was used as a measurement of how typical was the observed communication. By learning a model that was specific to each network, yet generalized to typical computer-to-computer traffic within and outside the network, a language model can identify sequences of network activity that are outliers concerning the model. They demonstrated positive unsupervised attack identification performance (AUC 0.84) on the ISCX IDS dataset which contains seven days of network activity with normal traffic and four distinct attack patterns.

G. Fernandes *et al.* [15] carried out a comprehensive survey on network anomaly detection. Their objective for this study was to review the most important aspects of anomaly detection, covering an overview of a background analysis as well as a core study on the most relevant techniques, methods, and systems within the area. Therefore, to ease the understanding of this survey's structure, the anomaly detection domain was reviewed under five dimensions: (1) network traffic anomalies, (2) network data types, (3) intrusion detection systems categories, (4) detection methods and systems, and (5) open issues. The paper concluded with an open issues summary discussing presently unsolved problems, and final remarks.

A. Nagaraja *et al.* [16] worked on similarity-based feature transformation for network anomaly detection where feature reduction was achieved using the proposed feature transformation technique. However, their approach for feature transformation used the proposed Gaussian distance function to achieve dimensionality reduction to represent the original input dataset in the new transformation space. They further proposed a new computation expression for determining equivalent deviation and threshold in Gaussian space. Experiments were performed on KDD and NSL-KDD datasets by considering widely applied classifier algorithms in various state-of-the-art research contributions. For

performance validation of machine learning models, k-fold cross-validation was applied by setting k to 10 by considering evaluation parameters such as accuracy, precision and recall. Experiment results proved that their approach for anomaly detection that applies the proposed feature transformation technique proved comparatively better than detection methods CANN, GARUDA, and UTTAMA addressed in the recent research literature.

ii) Deep Learning Approaches

S. Naseer *et al*. [17] in their work "Enhanced network anomaly detection based on deep neural networks" investigated the suitability of deep learning approaches for anomaly-based intrusion detection systems. For this research, they developed anomaly detection models based on different deep neural network structures, including convolutional neural networks, autoencoders, and recurrent neural networks. These deep models were trained on NSLKDD training data set and evaluated on both test datasets provided by NSLKDD, namely NSLKDDTest+ and NSLKDDTest21. All experiments in this paper were performed by authors on a GPU-based test bed. Conventional machine learning-based intrusion detection models were implemented using well-known classification techniques, including extreme learning machine, nearest neighbor, decision tree, random forest, support vector machine, naive bays, and quadratic discriminant analysis. Both deep and conventional machine learning models were evaluated using well-known classification metrics, including receiver operating characteristics, the area under the curve, precision-recall curve, mean average precision and accuracy of classification. Experimental results of deep IDS models showed promising results for real-world applications in anomaly detection systems.

A. H. Hamamoto *et al.* [18] in their research "Network anomaly detection system using genetic algorithm and fuzzy logic" developed a scheme combining Genetic Algorithm and Fuzzy Logic for network anomaly detection. The Genetic Algorithm was used to generate a Digital Signature of Network Segment using Flow Analysis, where information extracted from network flow data was used to predict the network traffic behavior for a given time interval. Furthermore, a Fuzzy Logic scheme was applied to decide whether an instance represents an anomaly or not, differing from some approaches present in the literature. Indeed, it was proposed an expert system with the capability to monitor the network's traffic with IP flows while expected behaviors are generated on a regular time interval basis, issuing alarms when a possible problem is present. The proposed anomaly detection system exposed network problems autonomously. The results acquired from applying the proposed approach in real network traffic flows achieve an accuracy of 96.53% and a false positive rate of 0.56%. Moreover, their method succeeded in achieving higher performance compared to several other approaches.

D. Kwon *et al*. [19] embarked on a survey of deep learning-based network anomaly detection. They presented an overview of deep learning methodologies, including restricted Bolzmann machine-based deep belief network, deep neural network, and recurrent neural network, as well as the machine learning techniques relevant to network anomaly detection. In addition, this article introduced the latest work that employed deep learning techniques with a focus on network anomaly detection through the extensive literature survey. They also discussed their local experiments showing the feasibility of the deep learning approach to network traffic analysis. M. Said *et al.* [20] proposed a network anomaly detection using LSTM based autoencoder. They proposed a hyper approach based on Long Short Term Memory (LSTM) autoencoder and One-class Support Vector Machine (OC-SVM) to detect anomaly-based attacks in an unbalanced dataset, by training the models using only examples of normal classes. The LSTM-autoencoder was trained to learn the normal traffic pattern and to learn the compressed representation of the input data (i.e. latent features) and then fed it to an OC-SVM approach. The hybrid model overcomes the shortcomings of the separate OC-SVM, which is its low capability to operate

with massive and high-dimensional datasets. Additionally, they performed their experiments using the most recent dataset (InSDN) of Intrusion Detection Systems (IDSs) for SDN environments. The experimental results showed that the proposed model provides a higher detection rate and reduces the processing time significantly. Hence, their method provided great confidence in securing SDN networks from malicious traffic.

B. Lindemann *et al*. [9] carried out a survey on anomaly detection for technical systems using LSTM networks. In their article, a survey on state-of-the-art anomaly detection was done using deep neural and especially long short-term memory networks. The investigated approaches were evaluated based on the application scenario, data and anomaly types as well as further metrics. To highlight the potential of upcoming anomaly detection techniques, graph-based and transfer learning approaches were also included in the survey, enabling the analysis of heterogeneous data as well as compensating for its shortage and improving the handling of dynamic processes. W. Xu *et al.* [21] worked on improving the performance of autoencoder-based network anomaly detection on NSL-KDD dataset. They proposed a novel 5-layer autoencoder (AE)-based model better suited for network anomaly detection tasks. Their proposal was based on the results they obtained through an extensive and rigorous investigation of several performance indicators involved in an AE model. In their proposed model, they used a new data pre-processing methodology that transforms and removes the most affected outliers from the input samples to reduce model bias caused by data imbalance across different data types in the feature set. The proposed model utilizes the most effective reconstruction error function which plays an essential role in the model to decide whether a network traffic sample is normal or anomalous. These sets of innovative approaches and the optimal model architecture allow their model to be better equipped for feature learning and dimension reduction thus producing better detection accuracy as well as F1-score. They evaluated their proposed model on the NSL-KDD dataset which outperformed other similar methods by achieving the highest accuracy and F1-score at 90.61% and 92.26% respectively in detection.

III. Methodology

In the pursuit of any scholarly investigation, the establishment of a robust research methodology serves as a fundamental pillar, orchestrating a systematic approach throughout the developmental trajectory. It delineates a structured pathway encompassing distinct phases, thereby shaping the proposed methodological framework. Within the specific purview of this study, the overarching aim is to devise a resilient and efficacious system for the detection of network intrusions. The envisaged research methodology is delineated into three principal phases: data preprocessing, feature selection, and classification and performance evaluation. The initial phase, data preprocessing, meticulously orchestrates the preparation and refinement of raw data to facilitate effective analysis. This involves intricate tasks such as handling missing values, normalizing data, and eliminating noise or outliers, with the primary objective of ensuring that the data is rendered in a format conducive to subsequent analysis.

Advancing further, the feature selection phase entails the discernment and extraction of pivotal attributes from the preprocessed data. The goal is to retain only those features wielding significant influence in the detection of network intrusions. To this end, the Linear Discriminant algorithm (LDA) is proposed, as it plays a crucial role in reducing dimensionality, enhancing model performance, and augmenting the interpretability of results. The concluding phase, classification and performance evaluation, leverages the features selected through the LDA algorithm to train machine learning classification models. Employing algorithms such as Random Forest and Support Vector Machine, the individual models undergo rigorous evaluation using metrics such as accuracy, precision, recall, and F1-score. This meticulous evaluation process ensures the reliability and efficacy of the models in discerning network intrusions. A visual representation of the proposed methodology is encapsulated in Fig. 1, providing a comprehensive overview of the sequential progression through the outlined phases. This methodological framework is structured not only to address the intricacies of network intrusion detection

but also to contribute valuable insights to the broader domain of cybersecurity research.

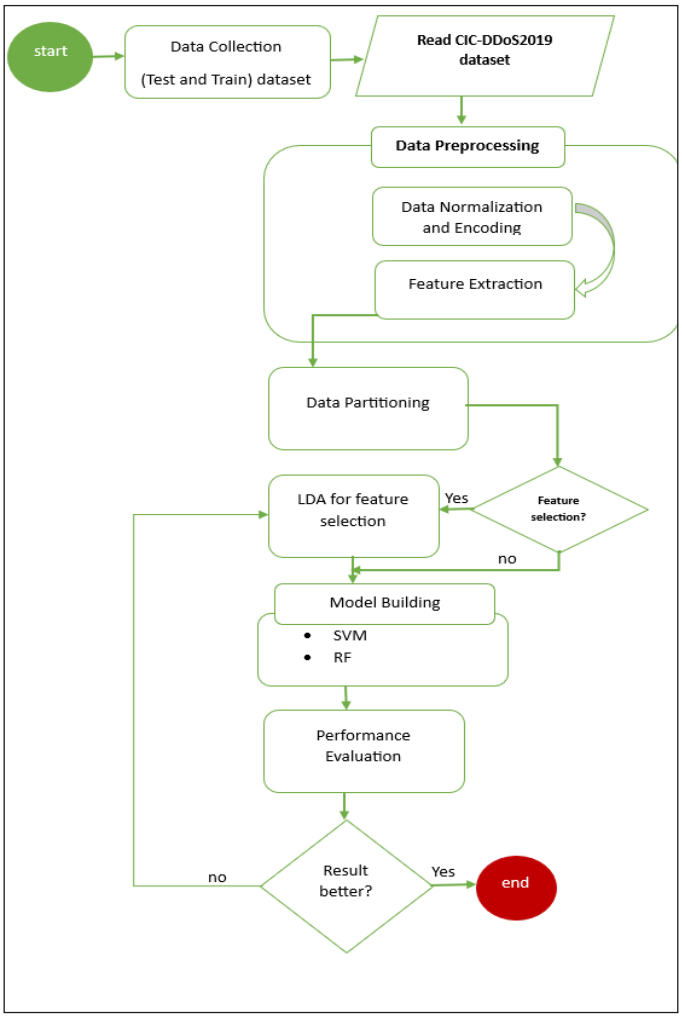


Fig. 1: The Model Flow Chart

A. Dataset Description

The dataset utilized to analyze network anomalies is the CIC-DDoS2019 dataset, provided by the Canadian Institute for Cybersecurity and obtained from the Mendeley machine learning repository. CIC-DDoS2019 comprises both benign and common DDoS attacks, making it representative of real-world network traffic (PCAPs). It includes labelled flows generated by CICFlowMeter-V3, indicating timestamps, source and destination IPs, ports, protocols, and attack types (stored in CSV files). The data was collected daily, with each day featuring raw network traffic (PCAPs) and event logs (Windows and Ubuntu event logs) per machine. The authors employed CICFlowMeter-V3 to extract over 80 traffic features from the raw data, saving them as CSV files per machine. The dataset encompasses various modern reflective DDoS attacks, such as PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP.

B. Data Preprocessing

In the proposed dataset, it was observed that certain attributes exhibit nominal values. Hence, it becomes imperative to convert these attributes into numerical values during both the training and testing phases. Algorithm 1, delineates the procedure for this conversion of nominal attributes into numerical values. Initially, the algorithm calculates the total count of nominal features. Subsequently, for each nominal feature, details such as the feature name, the number of variables (k), and the frequency of each variable within the feature are specified. Following this, the recurring variables are organized in descending order based on their occurrence frequency, and each variable is then assigned a numerical value ranging from zero to K.

Algorithm 1: Nominal to Numeric Algorithm
Step 1: nominal feature counter: *c*
Step 2: set $i = 1$
Step 3: while $i!$ = c **then**
Step 4: k_i = *num of variable (i) involved in feature C,* p_i*: num of repeated variable (i) repeated*
Step 5: Order repeated variable from maximum to minimum number
Step 6: allocate the number from zero to *k* that was obtained from step 2 to variables
Step 7: $i = i + 1$ goto step 3
Step 1: stop

C. Feature Selection

Feature selection is a methodology utilized to decrease the dimensionality of a feature set by eliminating extraneous features, thus preserving only the most salient ones. In the realm of DDoS detection, feature selection is implemented to optimize the efficiency of the detection process. The

aim is to discern and retain the most pertinent features while discarding those that do not substantially contribute to the detection task. Consequently, to identify the relevant features, the study advocated for the utilization of an artificial intelligence technique, specifically the LDA algorithm. Linear Discriminant Analysis (LDA) is a statistical method primarily used for dimensionality reduction and classification. In the context of feature selection, LDA operates by maximizing the separation between multiple classes or categories within the data [22]. It achieves this by projecting the feature space onto a lower-dimensional subspace, where the class separation is maximized [23]. Specifically, LDA identifies the directions (or linear combinations of features) that maximize the ratio of between-class variance to within-class variance. Features that contribute the most to this separation are retained, while those with less discriminatory power are discarded. By selecting features that effectively discriminate between classes, LDA facilitates the creation of a compact and informative feature set, which is essential for improving the performance of classification algorithms, such as in the case of network anomaly detection.

D. Classification Algorithm

The investigation into network anomaly detection utilizing the CIC-DDoS2019 dataset entails constructing and validating models using a supervised machine learning framework, particularly classification methods, given the dataset's classification challenge of network attacks. Primarily, the objective is to predict the class label of each sample based on the features present in the CIC-DDoS2019 dataset. Consequently, the study advocates for the utilization of various machine-learning techniques in model construction, including Random Forest (RF) and Support Vector Machine (SVM) algorithms.

E. SVM Algorithm

A Support Vector Machine (SVM) constructs hyperplanes in a high-dimensional space to facilitate classification, regression, or outlier detection. Its primary objective is to find an optimal linear hyperplane that maximizes the margin of separation between binary classes. This approach involves using a subset of the data to train the model, identifying support vectors that represent the training data, and utilizing these support vectors to classify unseen samples into target classes. In this study, an SVM model is developed to classify network anomalies as either normal or anomalous (indicative of an attack). When an intrusive connection occurs, the SVM model identifies the anomaly. The classification process involves using training and testing sets comprising instances of connections, where each instance includes a target value (normal or attack) and features identifying the entire instance [24]. Through SVM, this research constructs a model capable of predicting the presence or absence of a denial-of-service attack in the test set using a parameter configuration generated during model construction, training, and tuning. The SVM training algorithm, given a set of training samples belonging to two classes, builds a model that assigns new samples to one of the classes. It operates as a non-probabilistic binary classifier. By employing the kernel option, an SVM model can perform non-linear classification, albeit with a careful selection of parameters and kernels. In this work, the radial basis function kernel was utilized in tuning the model to generate the requisite parameters for SVM model construction.

F. Random Forest

Random Forest, an ensemble learning algorithm renowned for its robustness and accuracy in classification tasks, comprises multiple decision trees, each allowed to grow fully without the need for pruning. The essence of Random Forest lies in aggregating the predictions of these individual trees to produce a more precise and dependable outcome, effectively mitigating concerns of overfitting commonly encountered in machine learning. Notably, the algorithm possesses the inherent capability to automatically select relevant features during training, simplifying preprocessing steps and enhancing adaptability to diverse datasets. By utilizing random subsets of features for each decision tree, Random Forest fosters diversity among trees,

enabling comprehensive exploration of the feature space.

The application of Random Forest to network anomaly detection aims to address critical challenges in the field, particularly the accurate and reliable identification of anomalous activities or potential security threats within networks [25]. The collective decision-making process of multiple trees, each contributing unique insights, empowers the algorithm to effectively differentiate between normal and malicious network behaviour. Furthermore, its ability to provide an overall estimate enhances its utility in capturing intricate patterns associated with various cyber threats. The comprehensive analysis offered by Random Forest, stemming from the amalgamation of diverse decision trees, renders it well-suited for the nuanced landscape of network anomaly detection.

G. Performance Evaluation

To evaluate the performance of the RF and MLP model, the accuracy, precision, recall, and F1-score metrics are proposed. The criterion for each of the metrics is calculated according to four main criteria which are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) as follows:

- *True Positive (TP):* Indicates when an alarm is generated and there is an intrusion.
- *False Negative (FN):* Indicates when an alarm is not generated but there is an intrusion.
- *False Positive (FP):* Indicates when an alarm is generated but there is no intrusion.
- *True Negative (TN):* Indicates when an alarm is not generated and there is no intrusion.

Precision: Precision is a metric that focuses on the positive class and assesses how many of the predicted positives are true. It answers the question: "Of all the instances predicted as positive, how many were positive?". Equation (1) depicts the mathematical expression for the precision metrics.

$$precision = \frac{TP}{TP + FP} \tag{1}$$

Recall: Recall, also known as sensitivity or true positive rate, evaluates how many of the actual intrusion records were correctly predicted. It answers the question: "Of all the actual positives, how many were correctly predicted as positive?" The formula is shown in equation (2).

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

F-Measure (or F-Score): The F1 score is the harmonic mean of precision and recall. It provides a balanced evaluation of a classification model, taking into account both false positives and false negatives. It is particularly useful when dealing with imbalanced datasets. Equation (3) shows the mathematical formula for the F-score.

$$F - Measure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{3}$$

Accuracy: Accuracy is a commonly used metric to evaluate the overall performance of a classification model. It measures the proportion of correctly classified instances (both true positives and true negatives) out of the total number of instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

IV. Result and Discussion

A. Introduction

This chapter delineates the outcomes derived from a practical investigation and implementation focused on predicting network anomaly detection from the CIC-DDoS2019 dataset source from the Mendeley machine learning repositories. The research methodology encompasses the utilization of deep learning algorithms, namely the SVM and RF algorithm. Subsequently, the constructed models undergo comprehensive validation, assessing performance metrics such as precision, recall, and F1-score.

B. Parameter Settings

The parameters outlined in Table I, play a crucial role in configuring the RF and SVM models for network anomaly detection. In the context of machine learning algorithms like RF and SVM,

parameter settings play a critical role in determining the performance and behavior of the models. For the RF, the specified parameters include the choice of the kernel and the value of the random state, whereas for SVM, parameters such as the kernel type (in this case, Radial Basis Function or RBF), the regularization parameter C, and the random state are defined. Starting with the Random Forest algorithm, the parameter setting for the random state is set to 42. This parameter controls the randomness of the algorithm, ensuring reproducibility of results across different runs. By setting a specific random state, the algorithm's random number generator will produce the same sequence of pseudo-random numbers, leading to consistent results each time the model is trained. This is particularly important for debugging, testing, and comparing different models. Moving on to the SVM algorithm, the chosen kernel is the Radial Basis Function (RBF). The RBF kernel is a popular choice in SVM models due to its ability to capture complex relationships in the data, especially in cases where the decision boundary is non-linear. By using the RBF kernel, the SVM model can effectively handle datasets with non-linear decision boundaries, making it suitable for a wide range of classification tasks. Additionally, the regularization parameter C is set to 100. The regularization parameter C in SVM controls the trade-off between maximizing the margin and minimizing the classification error. A higher value of C indicates a smaller margin and a higher penalty for misclassification, leading to a more complex decision boundary that closely fits the training data. By setting C to 100, the SVM model prioritizes achieving high accuracy on the training data while still maintaining generalization capability on unseen data.

Table I: RF and SVM Model Parameter Setting

Parameter	Value
Kernel	RBF
C	100
Random State	42

Overall, these parameter settings reflect a combination that aims to strike a balance between effective learning, model convergence, and handling the characteristics of the data used in the network anomalies detection model. Fine-tuning and experimentation with these parameters may be necessary based on the specific characteristics of the dataset and the desired performance of the model in case of further research.In the development of a network anomaly detection model, a crucial step involves incorporating a dataset for training purposes. Subsequently, the identification of anomalous incidents within the dataset was carried out utilizing RF and SVM models. To facilitate this experimental process, the Pandas library was utilized for efficient dataset manipulation. Pandas, a widely-used Python library sourced externally, offers modules designed to streamline the ingestion of datasets in various file formats. In this particular study, the dataset was formatted as a CSV (Comma Separated Values) file. Notably, the 'read_csv' function within the Pandas library proved to be highly effective in assimilating and presenting dataset attributes in a tabular structure. This functionality significantly enhances the analytical framework of the investigation, enabling a more streamlined and organized approach to data analysis. Whereas, Fig. 2 displays the result of using the pandas read_csv function.

```
In [26]: df.head()
Out[26]:
```

ned: 0	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	...	Active Mean	Active Std	Active Max	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label	Class
0	17	216631	6	0	2088.0	0.0	393.0	321.0	348.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	UDP	Attack
1	17	2	2	0	802.0	0.0	401.0	401.0	401.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	UDP	Attack
2	17	48	2	0	766.0	0.0	383.0	383.0	383.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	UDP	Attack
3	17	107319	4	0	1398.0	0.0	369.0	330.0	349.5	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	UDP	Attack
4	17	107271	4	0	1438.0	0.0	389.0	330.0	359.5	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	UDP	Attack

80 columns

Fig. 2: Depict Records

C. Data Exploration

This module, serving as a section for data exploration, facilitates the visualization of select features within the dataset. The utilization of visualizations empowers the scientific inquiry to discern inherent patterns and interrelationships among distinct variables encapsulated within the dataset.

D. Dataset Descriptive Statistics

Conducting thorough analytical research is essential for obtaining a deep statistical understanding of data characteristics, which in turn enables the precise design and execution of optimal experiments. The tabular representation in Fig. 3 provides a clear depiction of data intervals at the 25th, 50th, and 75th percentiles, obtained using Panda's data frames. This tabulated format encompasses vital statistical metrics, including count, mean, standard deviation, minimum, and maximum values. The count column enumerates instances of network anomalies records, totaling 431,371. 'Min' denotes the minimum floating value, 'std' represents the standard deviation specific to each labelled column, and 'max' indicates the maximum values in the corresponding column. Each column is associated with its unique values for descriptive statistics, offering a comprehensive analytical portrayal.

```
: df.describe()
```

	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std
count	431371.000000	4.313710e+05	431371.000000	431371.000000	4.313710e+05	4.313710e+05	431371.000000	431371.000000	431371.000000	431371.000000
mean	13.948694	8.404856e+06	24.139117	2.472021	9.416956e+03	1.632896e+03	357.483674	294.721646	324.915327	20.208259
std	4.966712	2.126596e+07	195.888896	56.370208	3.445253e+04	1.064056e+05	320.025929	273.298705	268.577313	70.946085
min	0.000000	1.000000e+00	1.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	0.000000
25%	6.000000	7.870000e+02	4.000000	0.000000	7.800000e+01	0.000000e+00	37.000000	6.000000	32.000000	0.000000
50%	17.000000	4.480400e+04	4.000000	0.000000	2.064000e+03	0.000000e+00	440.000000	330.000000	428.000000	0.000000
75%	17.000000	3.002508e+06	16.000000	2.000000	5.160000e+03	0.000000e+00	516.000000	516.000000	516.000000	0.000000
max	17.000000	1.199987e+08	86666.000000	31700.000000	1.526642e+07	5.842950e+07	32120.000000	2131.000000	3015.290500	2221.556200

8 rows × 77 columns

Fig. 3: Descriptive Statistics

E. Data Scaling

Normalization, commonly known as data scaling, is a crucial step in data preprocessing that significantly impacts the performance of machine learning models. Its primary goal is to standardize the scale of all features or variables present in the network anomaly dataset. This process involves adjusting the numerical values associated with these features to adhere to a standardized floating-point distribution. By doing so, normalization ensures that all features contribute equally to the model's learning process, preventing the dominance of certain features due to their larger scales. The standardized distribution achieved through normalization enhances the predictive accuracy of the model, especially in the context of early network anomaly detection. By bringing all features to a comparable scale, the model can more effectively discern patterns and anomalies within the data, leading to improved detection capabilities. In this study, the implementation of feature scaling was strategically executed using the Standard Scaler module available within the Scikit-learn machine learning framework. This module offers optimized capabilities for scaling features, ensuring efficient and effective normalization of the dataset. The utilization of the Standard Scaler module illustrates its integral role in the preprocessing pipeline of the network anomaly detection system.

F. Feature Selection

As mentioned earlier, the study employed the LDA algorithm for feature selection on the CIC-

DDoS2019 network anomaly dataset. The selected features resulting from this process are presented in Fig. 4, which is a sample code output illustrating these selected features. The threshold for the selected features was set to 20 features.

```
[n [19]: top_20_features

)ut[19]: Index(['ACK Flag Count', 'CWE Flag Count', 'URG Flag Count', 'Down/Up Ratio',
                'SYN Flag Count', 'Label', 'Protocol', 'Fwd PSH Flags',
                'RST Flag Count', 'Packet Length Mean', 'Bwd Packet Length Min',
                'Avg Packet Size', 'Fwd Packet Length Std', 'Packet Length Std',
                'Bwd Packet Length Mean', 'Avg Bwd Segment Size', 'Subflow Bwd Packets',
                'Total Backward Packets', 'Avg Fwd Segment Size',
                'Fwd Packet Length Mean'],
               dtype='object')
```

Fig. 4: LDA Feature Selection Result

G. Data Balancing

To address the class imbalance within the CIC-DDoS2019 dataset, the SMOTE data augmentation technique was employed. The reason for the application of the SMOTE data balancing was because the class labels for the attack and benign are not balanced. Hence, the SMOTE approach aimed to create a more equitable distribution between attack and benign labels. As a result of applying the SMOTE algorithm, both attack and benign labels were balanced, with each totaling 333,540 instances. The augmentation process led to the generation of additional records.

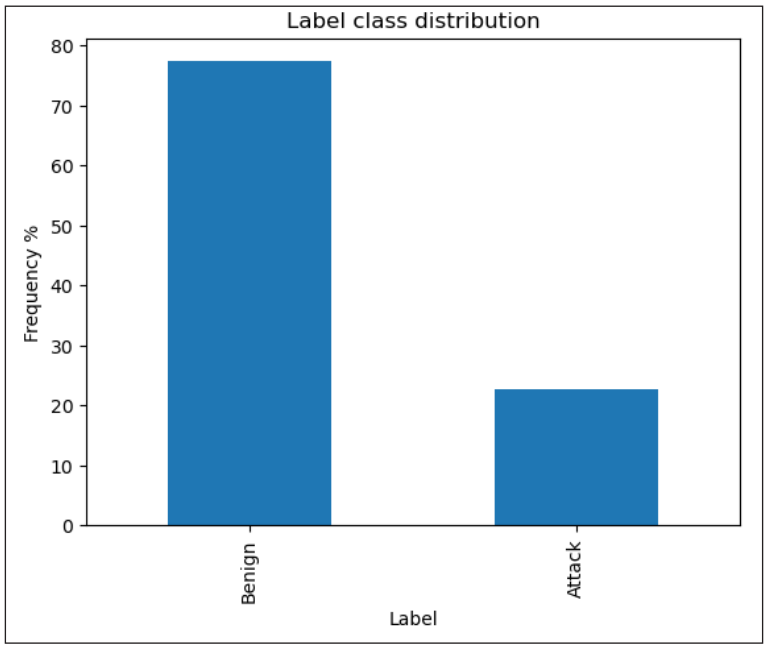


Fig. 5: Smote Data Balancing

H. Percentage Split Technique

To train the SVM and RF models, the dataset was divided into training and testing sets. The training set consisted of 70% of the total 431,371 network anomaly records, which were categorized into two classes. This training set was utilized to train the models effectively. The remaining 30% of the dataset was set aside for testing and validating the performance of the trained models.

I. Models Result

The performance of Support Vector Machine (SVM) and Random Forest (RF) models for network anomaly detection using the CIC-DDoS2019 dataset is presented in Table II. The Random Forest model achieved a training accuracy of 99.99% and a testing accuracy of 99.99%. This indicates that the RF model was able to effectively learn from the training data and generalize well to unseen data, achieving a high level of accuracy in detecting network anomalies. On the other hand, the SVM model achieved slightly lower performance with a training accuracy of 99.76% and a testing accuracy of 99.69%. While the SVM model also demonstrated strong performance, it fell slightly short compared to the RF model in terms of accuracy.

Table II: Network Anomalies Models Result (SVM and RF)

Models	Training Accuracy (%)	Testing Accuracy (%)
RF	1.0	99.99
SVM	99.76	99.69

Overall, both models performed well in detecting network anomalies, with the RF model exhibiting slightly better performance in terms of accuracy

J. Result Evaluation (Classification Report)

The SVM classification report for network anomaly detection using the CIC-DDoS2019 dataset indicates high performance across various evaluation metrics as shown in Fig. 6. With a precision of 0.9966 for class 0 and 0.9973 for class 1, the SVM demonstrates a strong ability to accurately classify instances of both normal and anomalous network traffic. Similarly, the recall scores of 0.9973 for class 0 and 0.9965 for class 1 indicate the model's effectiveness in identifying the majority of instances belonging to each class. The F1-scores, which consider both precision and recall, are also high for both classes, with values of 0.9970 for class 0 and 0.9969 for class 1. Moreover, the overall accuracy of the SVM model is reported as 0.9969, indicating its ability to correctly classify a large proportion of instances in the dataset.

```
 SVM Training Score: 0.9976788488569949
 SVM Test Score: 0.9969359571897117
SVM Classification Report:
              precision    recall  f1-score   support

           0     0.9966    0.9973    0.9970     23321
           1     0.9973    0.9965    0.9969     23023

    accuracy                         0.9969     46344
   macro avg     0.9969    0.9969    0.9969     46344
weighted avg     0.9969    0.9969    0.9969     46344

SVM AUC Score: 0.9969333329134069
```

Fig. 6: SVM Classification Report

The Random Forest classification results for network anomaly detection using the CIC-DDoS2019 dataset indicate exceptionally high-performance metrics as shown in Fig. 7. The precision, recall, and F1-score for both classes (0 and 1) are all very close to 1, indicating near-perfect classification accuracy. Specifically, for class 0, the precision, recall, and F1-score are all above 0.9996, while for class 1, they are all above 0.9996 as well. The overall accuracy of the model is reported to be 0.9998, which further emphasizes its effectiveness in accurately classifying network anomalies. The macro average and weighted average scores for precision, recall, and F1-score are also exceptionally high, all close to 0.9998.

```
 Random Forest Training Score: 1.0
 Random Forest Test Score: 0.9997842037116962
Random Forest Classification Report:
              precision    recall  f1-score   support

           0     0.9996    1.0000    0.9998      2256
           1     1.0000    0.9996    0.9998      2378

    accuracy                         0.9998      4634
   macro avg     0.9998    0.9998    0.9998      4634
weighted avg     0.9998    0.9998    0.9998      4634

Random Forest AUC Score: 0.9997897392767031
```

Fig. 7: RF Classification Report

In summary, these results suggest that both the SVM and RF models perform exceptionally well in detecting network anomalies in the CIC-DDoS2019 dataset, demonstrating high precision, recall, and accuracy across both normal and anomalous classes.

K. Result Evaluation (Receiver Operating Curve)

To comprehensively evaluate the effectiveness of the developed network anomaly detection models, the study employed the Receiver Operating Characteristic Area under the Curve (ROC-AUC) metric. ROC-AUC is a widely utilized metric for assessing classification model performance, especially in binary and multiclass scenarios. It gauges a model's ability to distinguish between positive and negative instances under varying threshold settings. The ROC-AUC curves depicted in Fig. 8 and Fig. 9 correspond to the SVM and RF models, and thus showcase the false positive rate (FPR) on the x-axis and the true positive rate (TPR) on the y-axis. TPR is synonymous with sensitivity or recall. The graphical representation elucidates the balance between TPR and FPR as the classification threshold undergoes variation. An optimal ROC-AUC curve resides in the top-left corner, indicating high sensitivity and low false positive rate, resulting in a larger area under the curve. Remarkably, the ROC-AUC metric for the SVM, and RF consistently achieved 99.99%, denoting impeccable discrimination between positive and negative instances. This signifies the models' robust performance in effectively identifying instances of network anomalies while minimizing false positives.

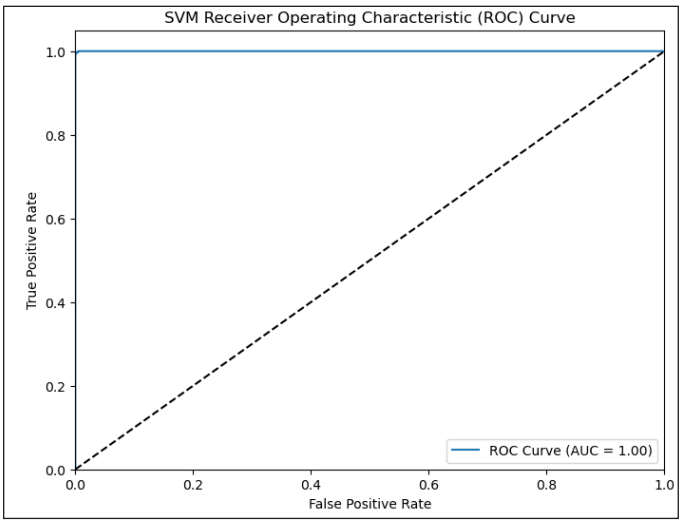


Fig. 8: SVM ROC-AUC Curve Graph

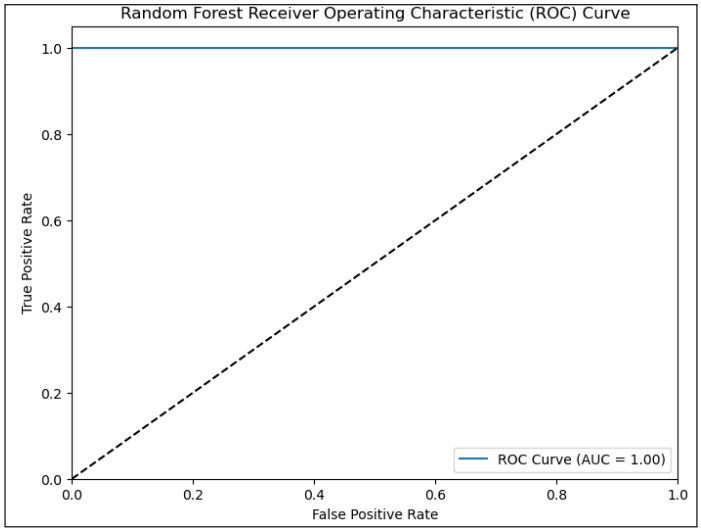


Fig. 9: RF ROC-AUC Curve Graph

In today's rapidly evolving digital environment, the proliferation of cyber threats poses a formidable challenge to the security of networked systems, a concern underscored by findings from our research survey. The urgent need to reinforce these systems against unauthorized access, data breaches, and other malicious activities emphasizes the critical importance of network anomaly detection. These models play a pivotal role in proactively identifying and mitigating potential threats by analyzing network traffic patterns, anomalous behaviours, and known attack signatures. Their deployment is indispensable for safeguarding sensitive information, preserving data integrity, and bolstering the overall resilience of interconnected infrastructures. As cyber threats continue to evolve, the ongoing development and refinement of network anomaly detection models emerge as imperative measures to outpace adversaries and uphold the security and reliability of digital networks.

To address these challenges, our study devised a systematic three-phase methodology for the development of network anomaly detection models. The initial phase involved meticulous data preparation, encompassing tasks such as the removal of unwanted characters, handling missing values, and feature selection using the LDA algorithm. Subsequently, the cleaned and

scaled dataset was inputted into machine learning algorithms, specifically SVM and RF, maintaining a 70:30 training-to-test ratio. The models underwent evaluation using precision, recall, accuracy, and F1-score metrics in the third phase of the methodology. Implementation of this research was facilitated through the utilization of the Python programming language, leveraging key third-party libraries including NumPy, Matplotlib, Pandas, TensorFlow, and Sklearn. This sequential methodology aimed to offer a structured and efficient framework for the development and evaluation of network anomaly detection models.

V. Conclusion

The study effectively developed and assessed the SVM and RF models for detecting network anomalies using the CIC-DDoS2019 dataset. The technique included feature selection by LDA, data balancing with the SMOTE algorithm, and dividing the dataset into training and testing subsets. Both models demonstrated strong performance in identifying network anomalies, with the RF model marginally surpassing the SVM model in accuracy. The RF model attained a training accuracy of 99.99% and a testing accuracy of 99.99%, whereas the SVM model reached a training accuracy of 99.76% and a testing accuracy of 99.69%. The classification results showed high precision, recall, and F1-score metrics for both models, suggesting their accurate ability to categorise regular and aberrant network traffic events. The ROC-AUC analysis verified the models' strong performance, continuously attaining 99.99% discrimination between positive and negative occurrences with very few false positives. Conclusively, the study results indicate that both SVM and RF models are successful in identifying network anomalies in the CIC-DDoS2019 dataset, demonstrating their practical utility in network security. Additional studies should investigate more feature engineering methods and model optimisations to improve efficiency and scalability in larger datasets and intricate network contexts.

A. Recommendation

This module provides prospective highlights for future application domains for the network anomaly detection model and thus identifies potential areas for advancing future research to enhance the efficacy of these models in detecting network anomalies. This exploration aims to provide insights into the broader applicability of the developed models and to suggest directions for continuous improvement in the field of network anomaly detection.

B. Application Areas

The developed network anomaly detection system exhibits significant potential for effective deployment in several key areas within the realm of cybersecurity. These areas include:

- *Enterprise Networks:* Implementing the system within enterprise networks can enhance overall cybersecurity posture by providing proactive detection and mitigation of potential network invasions. It contributes to safeguarding sensitive corporate data and maintaining the integrity of network infrastructure.
- *Critical Infrastructure Protection:* Deploying the network anomalies detection system in critical infrastructure sectors such as energy, transportation, and healthcare can bolster the security of essential services. It aids in preventing malicious activities that may pose threats to the reliable operation of critical systems.
- *Cloud Security:* Integrating the system into cloud environments will ensure the continuous monitoring and protection of cloud-based applications and services. It adds an extra layer of defence against unauthorized access and data breaches in cloud computing architectures.

C. Suggestions for Further Research

After an extensive experimental study and review of several kinds of literature relating to the developed

network anomalies detection models, this study suggests future research as follows:

- *Ensemble Approaches:* Future studies can investigate the potential of ensemble methods by combining the strengths of different models, such as KNN, Multilayer Perceptron, etc. Ensemble techniques, like stacking or bagging, could potentially improve overall performance by leveraging the complementary strengths of diverse models.
- *Dynamic Adaptability:* Future studies can also explore the development of network anomaly detection systems that dynamically adapt to evolving network environments. This could involve the integration of reinforcement learning or other adaptive techniques to enhance the system's ability to recognize novel network anomalies or intrusion patterns.

References

[1] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber-attacks using network traffic," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8852-8859, 2020.

[2] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78658-78700, 2021.

[3] O. N. Nyasore, P. Zavarsky, B. Swar, R. Naiyeju, and S. Dabra, "Deep packet inspection in industrial automation control system to mitigate attacks exploiting Modbus/TCP vulnerabilities," in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity),* IEEE, 2020, pp. 241-245.

[4] N. Elmrabit, F. Zhou, F. Li, and H. Zhou, "Evaluation of machine learning algorithms for anomaly detection," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* IEEE, Jun. 2020, pp. 1-8.

[5] A. Bommert, X. Sun, B. Bischl, J. Rahnenführer, and M. Lang, "Benchmark for filter methods for feature selection in high-dimensional classification data," *Computational Statistics & Data Analysis*, vol. 143, p. 106839, 2020.

[6] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, "Machine learning in network anomaly detection: A survey," *IEEE Access*, vol. 9, pp. 152379-152396, 2021.

[7] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.,* vol. 60, pp. 19-31, 2016.

[8] M. Usama *et al.*, "Unsupervised machine learning for networking: Techniques, applications and research challenges," 2017, arXiv preprint, arXiv:1709.06599.

[9] B. Lindemann, B. Maschler, N. Sahlab, and M. Weyrich, "A survey on anomaly detection for technical systems using LSTM networks," *Computers in Industry*, vol. 131, p. 103498, 2021.

[10] B. Venkatesh, and J. Anuradha, "A review of feature selection and its methods," *Cybernetics and Information Technologies*, vol. 19, no. 1, pp. 3-26, 2019.

[11] V. Bolón-Canedo, E. Ataer-Cansizoglu, D. Erdogmus, J. Kalpathy-Cramer, O. Fontenla-Romero, A. Alonso-Betanzos, and M. Chiang, "Dealing with inter-expert variability in retinopathy of prematurity: A machine learning approach," *Comput. Methods Progr. Biomed.*, vol. 122, no. 1, pp. 1-15, 2015.

[12] M. Nicolau, and J. McDermott, "Learning neural representations for network anomaly detection," *IEEE Transactions on Cybernetics*, vol. 49, no. 8, pp. 3074-3087, 2018.

[13] D. Kwon, K. Natarajan, S. C. Suh, H. Kim, and J. Kim, "An empirical study on network anomaly detection using convolutional neural networks," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS),* IEEE, 2018, pp. 1595-1598.

[14] B. J. Radford, L. M. Apolonio, A. J. Trias, and J. A. Simpson, "Network traffic anomaly detection using recurrent neural networks," 2018, arXiv preprint, arXiv:1803.10769.

[15] G. Fernandes, J. J. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, "A comprehensive survey on network anomaly detection," *Telecommunication Systems*, vol. 70, pp. 447-489, 2019.

[16] A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran, "Similarity based feature transformation for network anomaly detection," *IEEE Access*, vol. 8, pp. 39184-39196, 2020.

[17] S. Naseer, Y. Saleem, S. Khalid, M. K Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018.

[18] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença Jr, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, pp. 390-402, 2018.

[19] D. Kwon, H. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, vol. 22, pp. 949-961, 2019.

[20] M. Said Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "Network anomaly detection using LSTM based autoencoder," in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 2020, pp. 37-45.

[21] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving performance of autoencoder-based network anomaly detection on NSL-KDD dataset," *IEEE Access*, vol. 9, pp. 140136-140146, 2021.

[22] D. K Choubey, M. Kumar, V. Shukla, S. Tripathi, and V. K. Dhandhania, "Comparative analysis of classification methods with PCA and LDA for diabetes," *Current Diabetes Reviews*, vol. 16, no. 8, pp. 833-850, 2020.

[23] L. Yang, X. Liu, F. Nie, and Y. Liu, "Robust and efficient linear discriminant analysis with $L_{2,1}$-norm for feature selection," *IEEE Access*, vol. 8, pp. 44100-44110, 2020.

[24] D. Wang, and G. Xu, "Research on the detection of network intrusion prevention with SVM-based optimization algorithm," *Informatica*, vol. 44, no. 2, 2020.

[25] Z. Liu, N. Su, Y. Qin, J. Lu, and X. Li, "A deep random forest model on spark for network intrusion detection," *Mobile Information Systems*, pp. 1-16, 2020.

Journal of Network and Information Security
13 (1) 2025, 18-29
www.publishingindia.com/jnis

Predictive Modeling for Breast Cancer Detection using Transfer Learning and Comparative Study of Some Existing Models

Jyoti Lakhani[1*] and Garima Charan[2]
[1]Assistant Professor, Department of Computer Science, Maharaja Ganga Singh University, Bikaner, Rajasthan, India. Email: jyotilakhani@mgsubikaner.ac.in
[2]Research Scholar, Department of Computer Science, Maharaja Ganga Singh University, Bikaner, Rajasthan, India. Email: garimacharan77@gmail.com
[*]Corresponding Author

Abstract: In the present manuscript, a deep neural network based predictive model has been proposed for breast cancer detection in mammogram images. In this study transfer learning was used to six different pre-trained convolutional neural networks. These neural networks are further trained and fine-tuned to perform breast cancer classification task in order to detect malignant tumor. Results of this experiment suggest that ResNet50 is best suitable model than other five models used to detect tumor in mammogram images with 99.89% testing accuracy. An experimental study has also been performed to observe the accuracies of six models to identify malignant tumors. A class level accuracy of these models has been calculated and we observe that ResNet50 can classify both benign and malignant tumors with almost equal accuracies. Other five models classified benign samples effectively but failed to classify malignant tumors effectively. It is also observed that EfficientNet was the fastest model followed by ResNet50. The two main contributions of this paper is to achieve 99.89% testing accuracy by training used light weight model trained only for 25 epochs and use of whole images without any radiologists intervention. The limitation of this research is the use of a small custom dataset and use of generalized parameters and weights of IMAGENET1K_V1 for fine-tuning. The proposed light-weight limited layer transfer learning models can be used for further experimentation to improve efficiency of models by adjusting weights along with different segmentation techniques.

Keywords: Breast cancer, Classification, Deep learning, Fine tuning, Transfer learning.

I. Introduction

Breast cancer is the second leading cause of mortality worldwide [1]. Mammography screening is considered as a promising tool to early identification of malignant lesions in breast images. Performing mammography for medical diagnosis at early stage of the disease can be helpful to reduce mortality rates in patients [2]. Identification of breast cancer in digital mammography images is an object detection and recognition problem of computer vision. Evidences of research are available in this field however breast cancer diagnosis at early stages with significant accuracy is still in its initial stages. Studies reveal that detection of breast cancer from digital mammography observed average 86.9% sensitivity and average 88.93% of specificity [3]. Advancements in the field of deep learning and biomedical image processing can be a driving force for early detection of breast cancer with significant

accuracy. Studies reveal that deep learning based algorithms for breast cancer detection are producing encouraging outcomes [4-11].

Deep learning algorithms require a large amount of data to be trained. Biomedical deep learning researchers are facing limited access to official biomedical digital image datasets and benchmarking datasets as this field is recently developing. To cope up with this limitation researchers are using transfer learning, a sub area of deep learning. Transfer learning has potential to construct deep neural networks by utilizing an already existing neural network that is pre-trained on some other dataset not related to biomedical field. The transfer learning based neural networks initialize its weights according to is previous training to identify features like lines, corners, edges and, texture and apply these weights to the biomedical or some other problem. In the present study we have applied transfer learning approach to detect breast cancer lesions in mammograms.

Breast mammography classification is considered as a difficult research problem in the area of image classification. The main reason behind this is its small Region of Interest (ROI) which includes masses and lesions. The ROI in a mammogram is roughly 100 x 100 pixels in size which is a very small percentage of the entire image (roughly 4000 x 3000 pixels) [12]. To avoid space complexity issues, researchers pre-process (clip and annotate) the images and concentrate on ROI only [13-18]. But this approach is an overburden because identifying and clipping the ROI required radiologist's intervention. In the present study, we have we classified mammograms to detect malignancy without the requirement for human involvement using full mammography pictures and transfer learning.

II. Literature Review

In recent years Deep Learning has gained attention in the field of detection and classification of breast cancer in mammograms. Deep learning algorithms have ability to automatically detect promising features from biomedical images without need of a radiographer. Some deep learning algorithms employed on mammograms for breast cancer detection are convolutional neural network (CNN), recurrent neural network (RNN), capsule networks (CN) ensemble learning (EL) etc. Several studies are available in literature for detection of breast cancer using these methods [19]. In literature [20-24], researchers have used an automated method to detect breast cancer in mammograms using deep learning. Transfer learning is a proven method in literature for enhancing performance of deep learning models [25-28]. In these studies for transfer learning, the process of diagnosis is decomposed into three phases. Each of these phases is addressed by separate CNN and at each phase novel image features have learned which transferred to the next step. Subsequently, this trained network have fine-tuned on small targeted dataset of specific domain. These models yield higher accuracies and sensitivity as compared to the pre-trained model trained in isolation [29]. These algorithms focus on the concept of transfer learning in two modes: feature extractor and fine tuning [29]. A state-of-art review for early diagnosis of breast cancer has been performed in which multilayer perceptron (MLP) and convolutional neural networks were used for early detection of breast cancer [30]. Similar approach has been performed in [31] in which CNN and transfer learning has been used to classify breast cancer and achieved 95.50% accuracy and 97% AUC. This demonstrates the potential and effectiveness of transfer learning and deep learning techniques to improve the accuracy of classification of mammograms for breast cancer detection [29]. Encoders were also being used by researchers for breast cancer detection. A Faster RCNN was used by researchers to detect and classify and observed 95% AUC. YOLO is another modern technique to detect and classify breast cancer. YOLO is another modern technique to detect and classify breast cancer from whole breast images [32]. Researchers also use feed-forward CNN, ResNet50, InceptionV2 on INbreast and DDSM dataset. YOLO achieved an F-score of 98.02% on INbreast and 99.28% on DDSM [33]. The InceptionResNet-V2 model gave the best accuracy: 95.32% on INbreast dataset and 97.50% on DDSM dataset. The YOLO detector, Falconi *et al.* used transfer learning on NASNet and VGG16 with fine-tuning to classify mammograms and observed 90.0% accuracy on INbreast dataset [34]. Other researcher

uses a custom CNN architecture with optimized hyper-parameters and observed 96.53% [35]. Some extensive reviews on breast cancer detection using deep learning have been performed [36-38]. Table I presents an analysis of recently developed deep learning neural networks for breast cancer detection and classification.

Table I: Recent Studies Performed for using Deep Learning Neural Networks for Breast Cancer Detection and Classification

Year	Neural Network Architecture Used	Accuracy	References
2016	DNN	96.7%	[40]
2016	SNN	86%	[41]
2017	Deep CNN	82%	[42]
2017	SNN	79.5%	[43]
2017	Multitask DNN	82%	[44]
2017	Transfer Learning	90%	[45]
2018	ROI based CNN	97%	[46]
2018	InceptionV3	97.35%	[47]
2018	VGG16	97.12%	[47]
2018	ResNet50	97.27%	[47]
2018	Faster R-CNN	95%	[48]
2018	Deep Generative	89%	[49]
2019	CNN	93.24%	[50]
2019	DCNN, Alexnet	75%	[51]
2020	InceptionV3	79.6%	[52]
2020	GAN and CNN	80%	[53]
2020	MobileNet	84%	[54]
2020	AlexNet	98.53%	[55]
2021	CNN	91.2%	[56]
2022	CNN with fine tuning	99.96%	[57]

III. Material and Methods

A. Dataset

The present study was conducted using a modified DDSM [58] dataset called MiniDDSM. This is a collection of lightweight thumbnail images of breast cancer with three classes - Normal, Benign, and Malignant. Each class in the dataset is a group of 4 lossless JPEG images of each patient. This group of four images includes images of left and right breast and MLO and CC perspectives of breast of the patient.

B. Hardware and Software

For the training, validation, and testing phases, we used Google Colab for the Google Computer Engine backend (GPU) with Python 3 that was equipped with 12.7 GB RAM, 15.0 GB GPU RAM, and 78.2 GB Disk Storage. The experimentation is carried out using TorchVision 0.16.0.

C. Workflow of the Experimentation

A transfer learning based breast tumor classifier has been developed. As we are using a small dataset which is insufficient for a deep learning model, transfer learning plays the tackling role of this problem in our experiment. PyTorch version 2.1.0 was used to develop our classifier model. The workflow of the proposed classifier has five stages- pre-processing, segmentation, feature extraction, feature selection, and classification. For feature extraction a shape based evolutionary algorithm [59] was applied on the image dataset after applying Gabor Filters [60].

i) Pre-Processing

To reduce the complexity and to focus on the objective of the experiment i.e. classification of breast cancer tumor, we have removed normal instances from the dataset and images of benign and malignant tumor have been used in this experiment. Pre-Processing and augmentation of the images have been performed by using transformation functions. For augmentation, images are normalized and flipped horizontally and then cropped and reduce to 224 pixels in size. Finally, a 70:30 split has been performed on the dataset for further experimentation.

ii) Deep Neural Network Architecture

Deep neural networks (DNN) or deep networks mimic human brain and perform deep learning to

find hidden patterns from the given data using deep learning algorithms. DNNs are state-of -art methods for classification. In the proposed research we have used Convolutional Neural Network (CNN) based DNN model which extracts local and global features from the data.

Convolutional layer has been the prime component of the proposed DNN. In convolution layer, each pixel (*x, y*) of the input image $\mathbb{I}_{x,y}$ has been convolved and produced a feature map with the kernel $\mathbb{K}_{k1\,X\,k2}$. The convolutional output of the convolutional layer $\mathcal{L}$ and feature $\mathcal{F}$ for a pixel (*x, y*) of input image $\mathbb{I}_{x\,y}$ can be written as:

$$\mathbb{I}_{x,y} * \mathbb{K}_{k1\,X\,k2} = \sum_{i=0}^{k1-1}\sum_{j=0}^{k2-1}\mathbb{I}_{x-i,y-j} * \mathbb{K}_{i\,X\,j} \quad (1)$$

Final outcome after adding bias $\mathbb{B}_{\mathcal{L},\mathcal{F}}$ in equation 1 will be:

$$\mathcal{O}_{\mathcal{L},\mathcal{F}} = \left(\mathbb{I}_{x,y} * \mathbb{K}_{k1\,X\,k2}\right) + \mathbb{B}_{\mathcal{L},\mathcal{F}} \quad (2)$$

To overcome the linear outputs produced by neurons, non-linear activation functions such as Sigmoid, TanH, ReLU and Leaky-ReLU has been used. Each of these activation functions has its own advantages and limitations. Following equations show these used activation functions:

$$\sigma(x) = 1/(1 + e^{-x}) \quad (3)$$

Sigmoid activation function have vanishing-gradient problem with large computational complexity.

$$\tanh(x) = 2 * \sigma(x) - 1 \quad (4)$$

TanH can avoid vanishing-gradient problem of sigmoid activation function.

$$ReLU(x) = \max(0, x) \quad (5)$$

ReLU is the most popular activation function. It filters all negative values.

$$LeakyReLU(x) = \sigma(x) + \alpha\mathrm{ReLU(x)} \quad (6)$$

Here $\alpha\ in\ \alpha ReLU(x)$ is a pre-determined parameter. Leaky-ReLU is a modified form of ReLU activation function.

The convolutional layer outputs significant amount of feature information which increases the execution time of remaining layers of the neural network. To overcome this problem, subsampling (pooling) has been performed in which a down-sampling of features has been performed. Max-Pooling, Average Pooling, Mixed max-average pooling and Gated max-average pooling are some pooling methods.

Sometimes DNN suffer from overfitting problem where a DNN shows very good performance in testing phase but performance graph declines steeply during testing stage. A dropout method has been used to overcome overfitting problem. In this method, some random neurons have been purposefully dropped out.

At the end of the DNN, a fully connected layer has been added in which all the neurons of flat later are fully connected to the next layer.

$$y_k^{end} = \sum_{i=1}^{end-1} w_{k,i}^{end} o_i^{end-1} + \mathbb{B}_k^{end-1} \quad (7)$$

In the last decision layer softmax activation function or support vector machine has been used. In soft max layer, cross entropy loss is calculated as:

$$\mathcal{D}_k = -In(\overline{y_k}) \quad (8)$$

Where $\overline{y_k}$ can be written as:

$$\overline{y_k} = \frac{\exp(y_k^{end})}{\sum_{k=1}^{2}\exp(y_k^{end})} \quad (9)$$

Here k = {1,2} i.e. number of classes, 1 for benign and 2 for malignant.

The proposed deep network consists of several layers such as convolution layer, pooling layers, dense layers and recurrent layers. Each layer has its own functionality. Convolution layers are considered as a foundation layer in a deep network. These convolution layers extract significant features from the images. The pooling layers subsampled the feature maps discovered by the convolution layer and reduce spatial dimension of the data. It also helps in controlling over-fitting and reducing computational load. Dense layers are used in the deep network to classify the images using sampled feature maps. Dense layer is also called fully connected or fully linked layers.

In the current study, we have employed cross domain transfer learning, in which a pre-existing, pre-trained deep neural network is utilized to detect breast cancer

in the mammograms. For this purpose we have performed fine tuning of the deep neural network by making layer modifications and freezing the parameters of some layers. Six different pre-trained deep learning models are used in this experiment. These selected deep neural network models used in the proposed study are – ResNet50, EfficientNet B0, AlexNet, MobileNet_v2, VGG16 and DenseNet201. For each of these pre-trained deep learning models we have kept top layers frozen. The last intermediate layer and the output layer of these selected deep neural network models are kept unfrozen to fine tune parameters. Sigmoid activation function is used in the output layer as the addressed research problem is a binary classification problem.

The experiment has been initiated by using ResNet50 model first. Several trials have been conducted to determine appropriate parameters for fitting the ResNet50 model for classification of the breast cancer. A train-test split has been applied to the pre-processed images. Parameters used for fine tuning of the pre-trained ResNet50 model are given in Table II. Other five pre-trained models were also fine-tuned and fitted as done with ResNet50 model so that performance of these models can be evaluated in the same controlled parametric environment.The effectiveness of the models was evaluated using the cross entropy loss criterion. The suggested fine-tuned models were also a fitted using the stochastic gradient descent approach at a learning rate of 0.001. For this, at every seventh epoch, a decay LR scheduler was employed to adjust the learning rate by a factor of 0.1.

Table II: Fine Tuning and Fitting Parameters

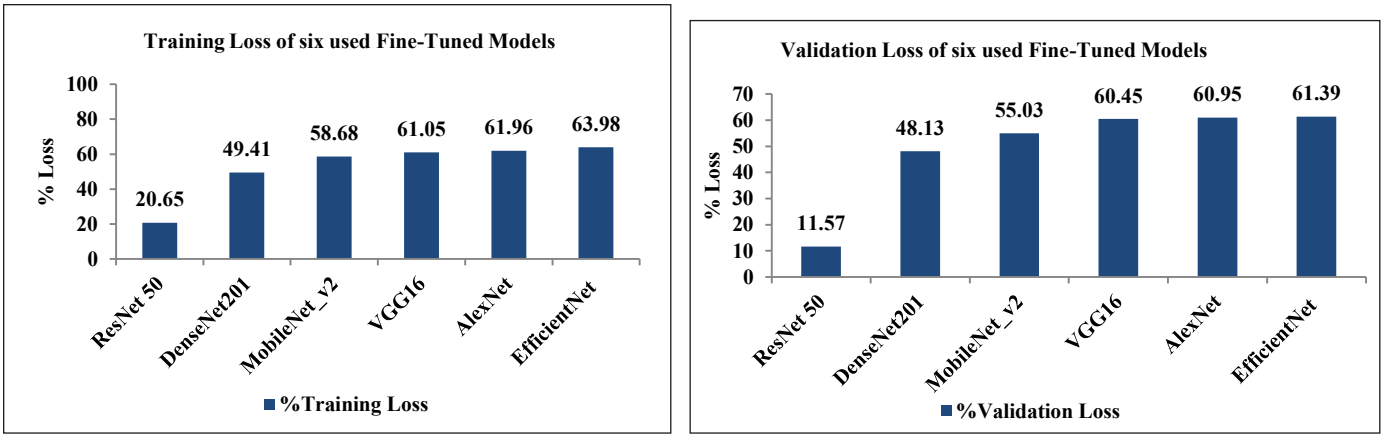
Optimizer	SGD
Learning Rate	0.001
Momentum	0.9
Loss Function	Cross Entropy Loss
Optimizer	SGD
From Logits	True
Metrics	Accuracy
Number of Epoch	25/50
Validation Steps	3/4

IV. Results and Discussion

A comparative performance analysis of six used deep neural network models has been done. All six fine tuned deep neural network models were executed for 25 epochs for training and validation purpose. In the training phase loss and accuracy of the model has been identified. After final epoch, the best model state has been identified which has highest accuracy throughout the training process. In the comparative performance analysis, the best performing states of six deep networks. The source code of this experimentation is publically available at Breast-Cancer-Classification-using-Transfer-Learning/.github/workflows at main · JyotiLakhani1/Breast-Cancer-Classification-using-Transfer-Learning

A. Losses

Fig. 1 is showing the average loss during the training and validation of six used deep neural networks. Training loss (%) of all six deep neural networks is shown in Fig. 1(a). ResNet50 has shown minimum training loss (20.65%) and EfficientNet has shown maximum training loss (63.98%). Performance loss observed during validation phase is observed in Fig. 1(b). In validation phase the EfficientNet has shown maximum validation loss (61.39%) and maximum ResNet50 has shown minimum validation loss (11.57%). It is clear that ResNet50 has shown minimum performance loss for both training and validation phase.

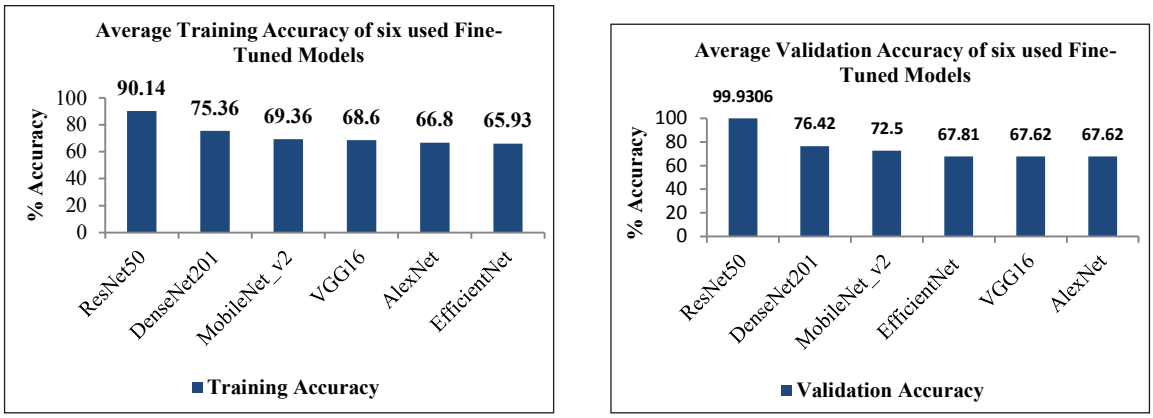


(a) (b)

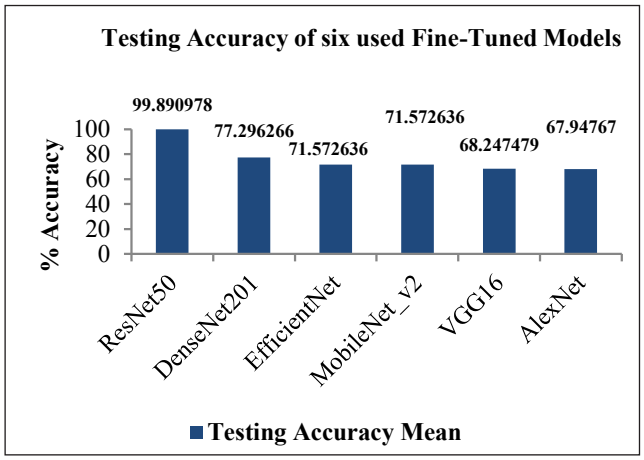
Fig. 1: Loss of the Six Fine-Tuned Deep Neural Network Models – (a) Average Training Loss Observed during Training Phase. The Comparison of Average Performance Loss at Training Phase of the Experimentation Observed ResNet50 < DenseNet201 < MobieNet_v2 < VGG16 < AlexNet < EfficientNet (b) Average Validation Loss Observed during Validation Phase. The Comparative Average Performance Loss at Validation Phase of the Experimentation Observed ResNet50 < DenseNet201 < MobieNet_v2 < VGG16 < AlexNet < EfficientNet

B. Accuracy

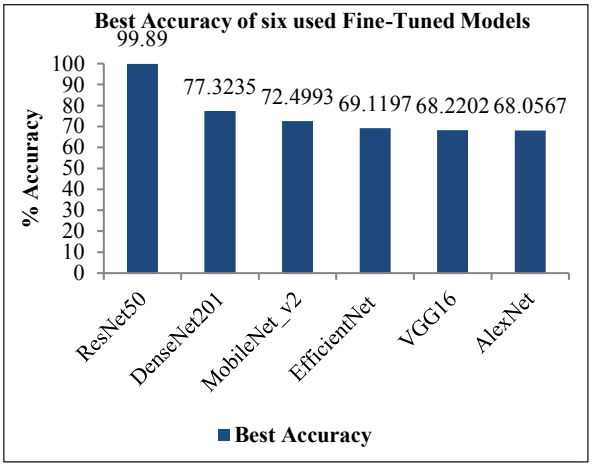
Average accuracy of six deep neural network models used for classification of breast cancer is shown in Fig. 2. Fig. 2(a) shows observed accuracy of used deep neural models at training phase of the experimentation. The ResNet50 model classify breast tumor with high accuracies. ResNet50 model demonstrates an average 90.14% training accuracy, 99.93% average validation accuracy and 99.89% average testing accuracy. The best accuracy shown by ResNet50 model is 99.89%. DenseNet is at the nest performer model. DenseNet shows 75.36% average training accuracy, 76.42% average validation accuracy, 77.29% average testing accuracy. It has shown 77.32% best accuracy during 25 epochs. EfficientNet stands last with 65.93% average accuracy in training phase but perform better in validation and testing phase with average 67.81% and 71.57% accuracy in the testing phase. Fig. 2(b) and Fig. 2(c) are showing comparative analysis of average accuracy of six pre-trained models used in the experiment during validation and testing phase. Fig. 2(d) is a comparative analysis of the best accuracy of the deep network models observed during execution. The best accuracy observed during the experiment is given by ResNet50 (99.89%) followed by DenseNet (77.32%) and EfficientNet (72.49%).



(a) (b)



(c)



(d)

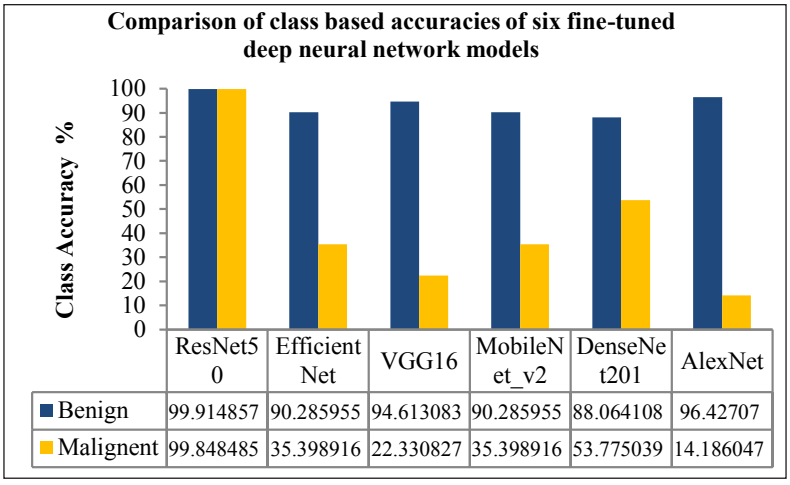
Fig. 2: Performance of the Six Fine-Tuned Deep Neural Models Observed – (a) Average Accuracies Observed during Training Phase. The Comparative Training Accuracies are ResNet50 > DenseNet201 > MobileNet_v2 > VGG16 < AlexNet < EfficientNet (b) Average Accuracies Observed during Validation Phase. The Comparative Validation Accuracies are ResNet50 > DenseNet201 > MobileNet_v2 > EfficientNet > VGG16 > AlexNet (c) Average Accuracies Observed during Testing Phase. The Comparative Analysis of Training Accuracies are ResNet50 > DenseNet201 > EfficientNet > MobileNet_v2 > VGG16 > AlexNet (d) Best Accuracies during an Epoch of the Execution of the Six Used Fine-Tuned Deep Neural Network Models. The Comparative Sequence of Performance of Best Accuracies are ResNet50 > DenseNet201 > MobileNet_v2 > EfficientNet > VGG16 > AlexNet

C. Class-Based Accuracy

It is important for a model to be unbiased and classify each class available in the dataset with same accuracy. An empirical study has been performed to evaluate the biasness and class based accuracies of the six used fine-tuned deep neural network models. The overall classification accuracies of six fine-tuned deep network models used in this experiment is shown in Fig. 3. The ResNet50 deep network shows no biasness and provides 99.91% for benign images and 99.84% accuracy for malignant images. This is an indication of a good classifier. The data in the Fig. 3 clearly indicate that other five deep network models performing well in classification of benign images but shown accuracy of identification of malignancy in mammogram less than 50%. This is an important factor if a researcher uses unbalanced datasets which have more images of benign lesions than the malignant in the dataset. In that case, other five deep network models may seem performing better than the ResNet50.

D. Other Performance Indicators

There are a number of other techniques available in literature to assess the performance of classification models. To evaluate the used models and to verify the results accuracy, sensitivity, and specificity of the used models have been calculated using True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). Total number of accurately detected benign and malignant breast tumors is known as True Positives (TP). The overall number of breast tumors diagnosed as malignant but turning out to be benign is known as False Positives (FP). The total number of cases that were correctly classified as benign is known as True Negative (TN).



	ResNet50	Efficient Net	VGG16	MobileNet_v2	DenseNet201	AlexNet
Benign	99.914857	90.285955	94.613083	90.285955	88.064108	96.42707
Malignent	99.848485	35.398916	22.330827	35.398916	53.775039	14.186047

Fig. 3: Overall Class-Based Accuracies of Used Fine-Tuned Deep Neural Network Models. Average Percentage of Accuracies Observed for Both Classes (Benign and Malignant) are Shown

The total number of images classified as benign but actually cancerous is known as False Negative (FN). Classification accuracy is a percentage of the total classification predictions that were correct. Accuracy is a measure of the efficiency of a classification model Eq.(1). Recall or sensitivity is a classification metric that assesses ability of a model to correctly identify the proportions of true positive predictions out of all predictions that are positive Eq.(2). Specificity is a metric that assesses the ability of model to identify true negative predictions among all negative outcomes Eq.(3). Precision also called Positive Precision Value (PPV), is a model performance metric that indicates probability of a model report a positive when it is actually positive Eq.(4). Negative Precision Value (NPV), is a model performance metric that indicates probability of a model report a negative when it is actually negative Eq.(5). F1-score is a statistical measure that rated the performance of the model. It is defined as the harmonic mean concerning precision and recall. Higher the value of F1-score suggests higher the performance of the model Eq.(6).

$$\text{Accuracy} = (TP + TN) + (TP + TN + FP + FN)\% \quad (1)$$

$$\text{Sensitivity} = TP / (FN + TP)\% \quad (2)$$

$$\text{Specificity} = TN / (FP + TN)\% \quad (3)$$

$$PPV = TP / (TP + FP)\% \quad (4)$$

$$NPV = TN/ (TN + FN) \quad (5)$$

$$\text{F1-score} = 2 * \frac{(\text{Precision} * \text{Recall})}{(\text{Precision} + \text{Recall})} \quad (6)$$

Table III is a comparison of performance indicators of six deep neural networks used in this study. These parameters clearly indicate that ResNet50 is performing better than all other models.

TABLE III: VARIOUS PERFORMANCE INDICATORS OF DEEP MODELS USED

Model	TN	TP	FP	FN	Sensitivity	Specificity	Precision PPV	NPV	F1
ResNet50	2347	1318	2	2	99.85	99.91	99.85	99.91	99.85
EfficientNet	2166	460	212	831	35.63	91.08	68.45	72.27	46.87
MobileNet_v2	2166	460	212	831	35.63	91.08	68.45	72.27	46.87
VGG16	2217	287	122	1043	21.58	94.78	70.17	68.00	33.00
AlexNet	2284	209	95	1081	16.20	96.00	68.75	67.87	26.22
DenseNet201	2097	739	274	559	56.9337	88.44	72.95	78.95	63.95

V. Conclusion

In this paper, a transfer learning based deep learning model for improving the classification of breast cancer in mammographic images was proposed. A modified mini-DDSM dataset is used for this study. This dataset consist of two classes benign and malignant. This dataset was pre-processed to remove noise and improving contrast. Data augmentation was performed to increase size of the dataset to enhance the performance of the six selected pre-trained deep neural network models. A random 70:30 training and testing split was applied on the used dataset. Freezing and fine-tuning techniques were used to calibrate the pre-trained deep neural network models for breast cancer classification task. ResNet50 is best suitable model than other five (VGG16, EfficientNet, DenseNet, AlexNet) to detect and classify breast cancer in mammogram image modality with 99.89% testing accuracy followed by DenseNet (77.29%), EfficientNet (71.57%), MobileNet_v2 (71.57%), VGG16 (68.25%) and AlexNet (67.95%). Class specific accuracies of each six models have also been calculated which state that ResNet50 classified both classes with equal accuracy (benign with 99.91% and malignant 99.84% accuracy). Surprisingly other five used models classified benign samples accurately but failed to detect malignancy in mammograms. It is also observed that EfficientNet was the fastest model followed by ResNet50. The two main contributions of this paper is to achieve 99.89% testing accuracy by training the model for only 25 epochs and use of whole images without any radiologists intervention. The limitation of this research is the use of a small custom dataset and use of only generalized parameters and weights of IMAGENET for fine-tuning of our transfer learning models. Implementation of the proposed transfer learning models on large datasets and fine tune them with different generalized weights may further improve the efficiency of the models. The proposed deep learning model can be further used other tumor identification problems.

References

[1] American Cancer Society, "How common is breast cancer?," 2018. Accessed: Jun. 12, 2024. [Online]. Available: https://www.cancer.org/cancer/breast-cancer/about/howcommon-isbreast-cancer.html

[2] K. C. Oefnger *et al.*, "Breast cancer screening for women at average risk: 2015 in guideline update from the American Cancer Society," *JAMA*, vol. 314, pp. 1599-1614, 2015.

[3] D. Constance Lehman *et al.*, "National performance benchmarks for modern screening digital mammography: Update from the Breast Cancer Surveillance Consortium," *Radiology*, vol. 283, no. 1, pp. 49-58, 2017.

[4] S. Sarah Aboutalib *et al.*, "Deep learning to distinguish recalled but benign mammography images in breast cancer screening," *Clinical Cancer Research*, vol. 24, no. 23, pp. 5902-5909, 2018.

[5] E.-K. Kim *et al.*, "Applying data-driven imaging biomarker in mammography for breast cancer screening: Preliminary study," *Scientific Reports,* vol. 8, no. 1, p. 2762, 2018.

[6] A. Hamidinekoo *et al.*, "Deep learning in mammography and breast histology, an overview and future trends," *Medical Image Analysis*, vol. 47, pp. 45-67, 2018.

[7] R. J. Burt *et al.*, "Deep learning beyond cats and dogs: Recent advances in diagnosing breast cancer with deep neural networks," *The British Journal of Radiology*, vol. 91, no. 1089, p. 20170545, 2018.

[8] T. Kooi *et al.*, "Large scale deep learning for computer aided detection of mammographic lesions," *Medical Image Analysis*, vol. 35, pp. 303-312, 2017.

[9] R. Agarwal *et al.*, "Automatic mass detection in mammograms using deep convolutional neural networks," *Journal of Medical Imaging,* vol. 6, no. 3, pp. 031409-031409, 2019.

[10] A. Rodriguez-Ruiz *et al.*, "Stand-alone artificial intelligence for breast cancer detection in mammography: Comparison with 101 radiologists," *NCI Journal of the National Cancer Institute*, vol. 111, no. 9, pp. 916-922, 2019.

[11] A. Rodríguez-Ruiz *et al.*, "Detection of breast cancer with mammography: Effect

of an artificial intelligence support system," *Radiology*, vol. 290, no. 2, pp. 305-314, 2019.

[12] S. Li *et al.*, "Deep learning to improve breast cancer detection on screening mammography," *Scientific Reports*, vol. 9, no. 1, p. 12495, 2019.

[13] T. Kooi *et al.*, "Large scale deep learning for computer aided detection of mammographic lesions," *Medical Image Analysis*, vol. 35, pp. 303-312, 2017.

[14] R. A. Jamieson *et al.*, "Breast image feature learning with adaptive deconvolutional networks," *Medical Imaging: Computer-Aided Diagnosis,* vol. 8315, 2012.

[15] J. Arevalo *et al.*, "Convolutional neural networks for mammography mass lesion classification," in *Proceedings of 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC, 2015)*, IEEE, 2015.

[16] J. Arevalo *et al.*, "Representation learning for mammography mass lesion classification with convolutional neural networks," *Computer Methods and Programs in Biomedicine,* vol. 127, pp. 248-257, 2016.

[17] D. Lévy, and A. Jain, "Breast mass classification from mammograms using deep convolutional neural networks," 2016, arXiv preprint, arXiv:1612.00542.

[18] N. Dhungel *et al.*, "The automated learning of deep features for breast mass classification from mammograms medical image computing and computer-assisted intervention (MICCAI) 2016," in *Proceedings of 19th International Conference,* Part II 19, Athens, Greece, Springer International Publishing, Oct. 17-21, 2016.

[19] L. Wang, "Mammography with deep learning for breast cancer detection," *Frontiers in Oncology*, 2024.

[20] H. Chougrad, H. Zouaki, and O. Alheyane, "Deep convolutional neural networks for breast cancer screening," *Computer Methods and Programs in Biomedicine,* vol. 157, pp. 19-30, 2018.

[21] D. Ribli, A. Horváth, Z. Unger, P. Pollner, and I. Csabai, "Detecting and classifying lesions in mammograms with deep learning," *Scientific Reports*, vol. 8, no. 1, p. 4165, 2018.

[22] Z. Q. Habeeb, B. Vuksanovic, and I. Q. Al-Zaydi, "Breast cancer detection using image processing and machine learning," *Journal of Image and Graphics*, vol. 11, no. 1, pp. 1-8, 2023.

[23] E. M. El Houby, and N. I. Yassin, "Malignant and nonmalignant classification of breast lesions in mammograms using convolutional neural networks," *Biomedical Signal Processing and Control*, vol. 70, p. 102954, 2021.

[24] L. Falconí, M. Pérez, W. Aguilar, and A. Conci, "Transfer learning and fine tuning in mammogram bi-rads classification," in *2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS),* IEEE, 2020, pp. 475-480.

[25] N. Laribi, D. Gaceb, A. Benmira, S. Bakiri, A. Tadrist, A. Rezoug, A. Titoun, and F. Touazi, "A progressive deep transfer learning for the diagnosis of Alzheimer's disease on brain MRI images," in *Artificial Intelligence: Theories and Applications: First International Conference* (*ICAITA*, 2022), Springer, 2023, pp. 65-78.

[26] M. Khaled, D. Gaceb, F. Touazi, A. Otsmane, and F. Boutoutaou, "Progressive and combined deep transfer learning for pneumonia diagnosis in chest x-ray images," in *Proceedings of the 5th International Conference on Informatics & Data-Driven Medicine,* Lyon, France, Nov. 18-20, 2022. CEUR Workshop Proceedings, vol. 3302, pp. 160-173, 2022.

[27] A. Yakoub, D. Gaceb, F. Touazi, and N. Bourahla, "Progressive deep transfer learning for accurate glaucoma detection in medical imaging," in *Proceedings of the 8th International Conference on Image and Signal Processing and Their Applications (ISPA, 2024)*, 2024.

[28] L. Chaouchi, D. Gaceb, F. Touazi, D. Djani, and A. Yakoub, "Application of deep transfer

learning in medical imaging for thyroid lesion diagnostic assistance," in *Proceedings of the 8th International Conference on Image and Signal Processing and Their Applications (ISPA, 2024)*, 2024.

[29] M. Khaled, F. Touazi, and D. Gaceb. "Improving breast cancer diagnosis in mammograms with progressive transfer learning and ensemble deep learning," *Arabian Journal for Science and Engineering,* 2024.

[30] M. Desai, and M. Shah, "An anatomization on breast cancer detection and diagnosis employing multi-layer perceptron neural network (MLP) and convolutional neural network (CNN)," *Clinical eHealth*, vol. 4, pp. 1-11, 2021.

[31] H. Chougrad, H. Zouaki, and O. Alheyane, "Deep convolutional neural networks for breast cancer screening," *Computer Methods and Programs in Biomedicine,* vol. 157, pp. 19-30, 2018.

[32] D. Ribli, A. Horváth, Z. Unger, P. Pollner, and I. Csabai, "Detecting and classifying lesions in mammograms with deep learning," *Scientific Reports*, vol. 8, no. 1, p. 4165, 2018.

[33] M. A. Al-Antari, S. M. Han, and T. S. Kim, "Evaluation of deep learning detection and classification towards computer-aided diagnosis of breast lesions in digital x-ray mammograms," *Computer Methods and Programs in Biomedicine,* vol. 196, p. 105584, 2020.

[34] L. Falconí, M. Pérez, W. Aguilar, and A. Conci, "Transfer learning and fine tuning in mammogram bi-rads classification," in *2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)*, IEEE, 2020, pp. 475-480.

[35] R. Karthiga, K. Narasimhan, and R. Amirtharajan, "Diagnosis of breast cancer for modern mammography using artificial intelligence," *Mathematics and Computers in Simulation,* vol. 202, pp. 316-330, 2022.

[36] R. M. Al-Tam, and S. M. Narangale, "Breast cancer detection and diagnosis using machine learning: A survey," *Journal of Scientific Research,* vol. 65, no. 5, pp. 265-285, 2021.

[37] G. Meenalochinia, and S. Ramkumar, "Survey of machine learning algorithms for breast cancer detection using mammogram images," *Materials Today*, vol. 37, no. 2, pp. 2738-2743, 2021.

[38] R. K. Yadav, S. Pardeep, and P. Kashtriya, "Diagnosis of breast cancer using machine learning techniques - A survey," *Procedia Computer Science*, vol. 218, pp. 1434-1443, 2023.

[39] Z. Jiao, X. Gao, Y. Wang, and J. Li, "A deep feature based framework for breast masses classification," *Neurocomputing*, vol. 197, pp. 221-231, 2016.

[40] B. Q. Huynh, H. Li, and M. L. Giger, "Digital mammographic tumor classification using transfer learning from deep convolutional neural networks," *Journal of Medical Imaging*, vol. 3, no. 3, p. 034501, 2016.

[41] W. Sun, T. L. Tseng, J. Zhang, and W. Qian, "Enhancing deep convolutional neural network scheme for breast cancer diagnosis with unlabeled data," *Computerized Medical Imaging and Graphics*, vol. 57, pp. 4-9, 2017.

[42] I. Kumar, H. S. Bhadauria, J. Virmani, and S. Thakur, "A classification framework for prediction of breast density using an ensemble of neural network classifiers," *Biocybernetics and Biomedical Engineering*, vol. 37, no. 1, pp. 217-228, 2017.

[43] N. Dhungel, G. Carneiro, and A. P. Bradley, "A deep learning approach for the analysis of masses in mammograms with minimal user intervention," *Medical Image Analysis*, vol. 37, 114-128, 2017.

[44] R. K. Samala, H. P. Chan, L. M. Hadjiiski, M. A. Helvie, K. Cha, and C. Richter. "Multi-task transfer learning deep convolutional neural network: Application to computer aided diagnosis of breast cancer on mammograms," *Physics in Medicine & Biology,* vol. 62, no. 23, pp. 8894-8908, 2017.

[45] M. A. Al-Masni, M. A. Al-Antari, J. M. Park, G. Gi, T. Y. Kim, P. Rivera *et al.*, "Simultaneous detection and classification of breast masses

in digital mammograms via a deep learning YOLO-based CAD system," *Computer Methods and Programs in Biomedicine*, vol. 157, pp. 85-94, 2018.

[46] H. Chougrad, H. Zouaki, and Q. Alheyane, "Deep convolutional neural networks for breast cancer screening," *Computer Methods and Programs in Biomedicine*, vol. 157, p. 19-30, 2018.

[47] D. Ribli, A. Horváth, Z. Unger, P. Pollner, and I. Csabai. "Detecting and classifying lesions in mammograms with deep learning," *Scientific Reports,* vol. 8, no. 1, p. 4165, 2018.

[48] R. Touahri, N. Azizi, N. E. Hammami, M. Aldwairi, and F. Benaida, "Automated breast tumor diagnosis using local binary patterns (LBP) based on deep learning classification," in *Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS),* Sakaka, Saudi Arabia, IEEE, 2019, pp. 1-5.

[49] A. S. Abdel Rahman, S. B. Belhaouari, A. Bouzerdoum, H. Baali, T. Alam and A. M. Eldaraa, "Breast mass tumor classification using deep learning," in *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT),* Doha, Qatar, IEEE, 2020, pp. 271-276.

[50] S. Shams, R. Platania, J. Zhang, J. Kim, K. Lee, and S. J. Park, "Deep generative breast cancer screening and diagnosis," in *Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention*, Granada, Spain, Springer, 2018, vol. 11071, pp. 859-867.

[51] L. Tsochatzidis, L. Costaridou, and I. Pratikakis, "Deep learning for breast cancer diagnosis from mammograms - A comparative study," *Journal of Imaging*, vol. 5, no. 37, 2019.

[52] N. Saffari, H. A. Rashwan, M. Abdel-Nasser, V. K. Singh, and D. Puig, "Fully automated breast density segmentation and classification using deep learning," *Diagnostics*, vol. 10, no. 11, p. 988, 2020.

[53] L. G. Falconi, M. Perez, W. G. Aguilar, and A. Conci, "Transfer learning and fine tuning in breast mammogram abnormalities classification on CBIS-DDSM database," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, pp. 154-165, 2020.

[54] A. H. Shayma'a, M. S. Sayed, M. L. Abdalla, and M. A. Rashwan, "Breast cancer masses classification using deep convolutional neural networks and transfer learning," *Multimedia Tools and Applications*, vol. 79, pp. 30735-30768, 2020.

[55] E. M. F. El Houby, and N. I. R. Yassin, "Malignant and nonmalignant classification of breast lesions in mammograms using convolutional neural networks," *Biomedical Signal Processing and Control*, vol. 70, p. 102954, 2021.

[56] V. Mudeng, J.-W. Jeong, and S.-W. Choe, "Simply fine-tuned deep learning-based classification for breast cancer with mammograms," *Computers, Materials and Continua*, vol. 73, no. 3, pp. 4677-4693, 2022.

[57] C. D. Lekamlage *et al.*, "Mini-DDSM: Mammography-based automatic age estimation," in *Proceeding of 3rd International Conference on Digital Medicine and Image Processing,* 2020.

[58] C. Bhuvaneswari, C. P. Aruna, and D. Loganathan, "A novel shape based feature extraction technique for diagnosis of lung diseases using evolutionary approach," *ICTACT Journal on Soft Computing,* vol. 4, no. 4, 2014.

[59] R. Mehrotra, N. K. Rao, and R. Nagarajan, "Gabor filter-based edge detection," *Pattern Recognition*, vol. 25, no. 12, pp. 1479-1494, 1992.

Journal of Network and Information Security
13 (1) 2025, 30-38
www.publishingindia.com/jnis

Optimized LTE-V2X Resource Allocation for Efficient V2V Communication in VANETs

Mamta Chauhan[1*], Rani Astya[2] and Nitin Rakesh[3]
[1]Department of Computer Science and Engineering (SET), Sharda University, Greater Noida, Uttar Pradesh, India. Email: mamta.gbu.ict@gmail.com
[2]Department of Computer Science and Engineering (SET), Sharda University, Greater Noida, Uttar Pradesh, India.
[3]Department of Computer Engineering & Technology, Symbiosis Institute of Technology, Nagpur Symbiosis International Deemed University, Pune, Maharashtra, India.
[*]Corresponding Author

Abstract: In Vehicular Ad-Hoc Networks (VANETs) play a crucial role in modern Intelligent Transportation Systems (ITS) by enabling real-time Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Long-Term Evolution for Vehicle-to-Everything (LTE-V2X) communication, particularly using the LTE-V2X side-link mode known as PC5 Mode, provides improved coverage, lower latency, and enhanced reliability compared to traditional Dedicated Short-Range Communication (DSRC)-based systems. However, existing LTE-V2X implementations face major challenges such as inefficient resource allocation, network congestion, high transmission delays, and security vulnerabilities. This research presents the Optimized Long-Term Evolution for Vehicle-to-Everything Resource Sharing (OLRS) framework, which integrates adaptive resource allocation, dynamic power control, and multi-hop emergency message forwarding with security-enhanced communication mechanisms. The proposed framework utilizes Roadside Unit (RSU)-assisted congestion management to prioritize safety-critical messages, such as emergency alerts, and ensures secure, efficient, and scalable data exchange between vehicles. By optimizing power control, spectrum allocation, and emergency message dissemination, OLRS significantly improves key network performance metrics, achieving a 40% reduction in latency, a 10% increase in Packet Delivery Ratio (PDR), and enhanced Signal-to-Interference-plus-Noise Ratio (SINR). The framework was implemented and tested using Cisco Packet Tracer for network simulation and Wireshark for real-time packet analysis. The results demonstrate improved data throughput, enhanced communication reliability, and stronger security against cyber threats. The proposed model provides a practical and scalable solution for high-density vehicular networks, with direct applications in collision avoidance, autonomous driving coordination, and intelligent traffic management.

Keywords: Cisco packet tracer, Cyber security, Long-term evolution for vehicle to everything, Resource allocation, Spectrum management, Vehicle to Vehicle communication, Vehicular ad hoc networks, Wire shark.

I. Introduction

Vehicular Ad Hoc Networks (VANETs) have emerged as a crucial component of Intelligent Transportation Systems (ITS), enabling seamless communication between vehicles and infrastructure. By facilitating real-time data exchange, VANETs

improve road safety, optimize traffic flow, and support autonomous driving. Among different V2V communication technologies, Dedicated Short-Range Communication (DSRC) and LTE-V2X have been widely explored. While DSRC operates on the IEEE 802.11p standard, it suffers from limited scalability, high interference, and congestion in dense vehicular environments. LTE-V2X, introduced in 3GPP Release 14, provides a more robust solution with better coverage, lower latency, and improved reliability, making it ideal for mission-critical vehicular applications. However, despite its advantages, LTE-V2X faces significant challenges in ensuring low-latency, high-throughput, and secure V2V communication. With the increasing number of connected vehicles, network congestion, inefficient resource allocation, high transmission delays, and security vulnerabilities have become major obstacles. When conventional LTE-V2X systems utilize pre-set resource assignments they experience wasted spectrum potential alongside deteriorating the reliability of message exchanges. The network performance suffers deterioration because dynamic power control mechanisms are absent thus leading to poor SINR (Signal-to-Interference-Noise Ratio). Real-time emergency alert dissemination becomes impaired because multi-hop communication remains inadequately developed.

The successful operation of V2V communication relies on achieving both efficient operation and real-time security in modern vehicular networks. Reliable vehicle-to-vehicle communication technology serves as the backbone forautonomous vehicles and smart transportation systems that help decrease traffic-related hazards as well as enhance traffic system efficiency and activate intelligent traffic management systems. The existing LTE-V2X systems face scalability problems requiring a new framework to optimize resource facilities and power management systems and data transmission security protocols. An Optimized LTE-V2X Resource Sharing (OLRS) framework serves as a proposed solution by utilizing adaptive scheduling methods to dynamically allocate resources for spectrum optimization with congestion reduction benefits. Safe communication alerts propagate through multiple hops more effectively because this system improves both emergency alert reliability and speed at the same time it implements encryption and authentication security methods to secure vehicle-to-vehicle transmission communications. The adaptive power control function of OLRS improves the SINR by adjusting transmitter powers for maximum efficiency and minimum interference. Analysis of the outlined framework happens through Cisco Packet Tracer and Wireshark tests whichdeliver practical results that go beyond simulations based on NS3 and SUMO.

Through its framework the proposed design advances multiple practical vehicular implementations specifically collision avoidance systems which help decrease accident frequency through quicker and better emergency message communications. Intelligent traffic management becomes possible through OLRS because it enables real-time congestion analysis which results in improved urban mobility through dynamic traffic rerouting. The framework allows autonomous vehicle coordination through its support of low-latency V2V communication which results in improved safety and efficiency of self-driving functions. Secure data exchange is strengthened because this work develops protective mechanisms using encrypted and authenticated V2V transmissions to safeguard vehicular networks from cyberattacks. This research addresses crucial downsides of current LTE-V2X technologies which supports the creation of future vehicle communication systems leading to improved vehicle network security and transportation efficiency.

II. Related Work

Several studies have focused on Vehicle-to-Vehicle (V2V) communication and resource-sharing techniques to enhance the efficiency, reliability, and security of Intelligent Transportation Systems (ITS) [1]. Traditional Wi-Fi-based V2V communication relies on Dedicated Short-Range Communi- cation (DSRC) or IEEE 802.11p, which offers low-latency communication but suffers from high interference, network congestion, and limited scalability in dense traffic conditions [2]. Due to the short transmission range and lack of centralized control DSRC-based communication becomes inefficient in high-mobility

environments, making LTE-V2X a more viable solution [3]. LTE-V2X and Resource Allocation Strategies with the introduction of 3GPP Release 14, LTE-V2X has emerged as a superior alternative to DSRC, providing direct V2V communication via the PC5 sidelink interface. LTE-V2X leverages cellular infrastructure and spectrum efficiency to support high-speed vehicular networks with better coverage and reduced interference. Several studies have proposed Device-to-Device (D2D) communication as a technique to enhance spectrum reuse and reduce network congestion by enabling vehicles to communicate without direct base station involvement [4]. One of the major research areas in LTE-V2X is resource allocation optimization. Different techniques, including reinforcement learning-based algorithms, power control strategies and QoS-aware scheduling mechanisms, have been proposed to improve throughput, reduce latency, and enhance spectrum efficiency. Some approaches focus on dynamic spectrum sharing, where V2V communication coexists with traditional cellular traffic by allocating radio resources adaptively based on traffic load and channel conditions [5]. Power allocation techniques, such as adaptive transmission power control and SINR-based allocation, have also been explored to improve Signal-to-Interference-Noise Ratio (SINR) and network reliability. Multi-Hop Communication and Emergency Message Dissemination. A critical component of V2V communication is the efficient propagation of emergency messages, particularly in accident scenarios where timely delivery of alerts can prevent secondary collisions [6]. Traditional methods rely on single-hop broadcasting, which limits the communication range. Multi-hop communication protocols have been established in literature that enables emergency messages to travel through numerous vehicles until they find their target receivers [6]. Emergency message delivery receives a higher priority in investigations that focus on priority-based message forwarding systems for faster delivery rates. Other methods apply RSU-assisted forwarding which enables Roadside Units (RSUs) to increase V2V message reachability outside immediate direct connection range [7]. The literature presents research about geocast and opportunistic forwarding algorithms that adapt message paths using network topology information andvehicle population levels. The implementation of V2V communication faces two significant security obstacles which require solutions for privacy and confidentiality protection. The three principal threats which affect V2V networks include eaves dropping attacks followed by spoofing incidents then Man-in-the-Middle (MITM) attacks [8]. The research community has investigated security solutions based on authentication protocols and cryptographic encryption schemes as well as intrusion detection systems (IDS). Special encryption methods have been created for vehicle communications while maintaining minimal computational costs. Two proposed authentication frameworks known as PKI and group-based authentication can verify vehicles to allow communication between them [9]. Studies have applied machine learning-based anomaly detection systems to track network activity patterns for stopping unauthorized access and detecting suspicious behavior within V2X communication networks. Studies have investing-gated blockchain technology for securing V2V data integrity by preventing unauthorized modification of V2V messages [10]. The most research said on LTE-V2X and V2V communication has relied on NS3, SUMO and OMNeT++ simulations to evaluate network performance under different traffic scenarios. While these simulation environments provide valuable insights, they do not fully reflect real-world implementation challenges [11]. Some works have attempted hardware-based testing using software-defined radios (SDRs) and vehicular test beds however, these solutions are often expensive and require specialized infrastructure.

III. Background Knowledge

Various approaches have been explored to optimize VANET communication using LTE.

- *5G-NR-V2X RSUs for Reliability:* Cooperative resource management for V2X using roadside units (RSUs) enhances network reliability and reduces shadowing effects [13].
- *LTE-V2X Direct Communication:* LTE-V2X sidelink modes (PC5) enable autonomous

resource allocation in V2V communication, particularly Mode 4, which allows vehicles to communicate without relying on network coverage [14].

- *Edge and Fog Computing in VANETs:* The integration of edge computing significantly improves real-time processing efficiency, reducing latency and improving network scalability.
- *Security Risks in V2V Communication:* Studies have shown that Wi-Fi-based V2V communication is prone to GPS spoofing, denial-of-service (DoS) attacks, and MITM vulnerabilities [1], [15].

While these studies focus on various aspects of VANET-LTE communication, there remains a need for a simple and effective method to establish direct V2V links, optimize resource distribution, and ensure security against network-based attacks using Cisco Packet Tracer.

IV. Methodology

The proposed methodology involves setting up an LTE-based V2V communication framework in Cisco Packet Tracer and analyzing traffic performance using Wireshark. The steps include:

Step 1: Network Topology Design

- Configure LTE-enabled vehicles as network nodes.
- Establish direct V2V communication channels.
- Implement mobility models to simulate real-world traffic.
- Simulate cyberattack scenarios to assess vulnerabilities.

Step 2: Packet Transmission Protocol

- Use LTE-V2X sidelink (PC5) mode for direct communication.
- Define message scheduling and transmission intervals.
- Implement access control mechanisms to prevent unauthorized access.

Step 3: Performance & Security Analysis

- Capture packet exchanges using Wire shark.
- Evaluate metrics including latency, throughput, and packet delivery ratio (PDR).
- Conduct penetration testing to identify vulnerabilities and propose countermeasures.

Step 4: Security Risks and Countermeasures

Table I: Security Risks

Security Threat	Description	Proposed Countermeasure
Eaves-dropping	Unauthorized interception of data	End-to-end encryption (AES-256)
Spoofing	Attackers impersonate legitimate vehicles	Secure authentication mechanisms (PKI)
DoS Attacks	Flooding network with fake messages	Rate limiting & anomaly detection
MITM Attacks	Intercepting and altering communication	TLS/SSL-based encrypted channels
GPS Spoofing	Sending false GPS signals to mislead vehicles	Multi-source GPS verification

A. Neighbor Discovery (How Vehicles Connect to Each Other?)

Technique ensures seamless V2V connectivity, emergency alert transmission, and efficient notification dissemination through the following mechanisms. Each vehicle periodically broadcasts hello messages using LTE-V2X sidelink (PC5 Mode 4) to discover nearby vehicles Steps:

Step 1: Vehicle Scanning: Each vehicle continuously scans its surroundings to detect nearby vehicles within its communication range.

Step 2: Beacon Messaging: Vehicles exchange periodic beacon messages containing:

- Vehicle ID (Unique identifier).
- Current Position (GPS Coordinates).
- Speed and Direction.
- Communication Status.

Step 3: Neighbor Table Update: Vehicles maintain an active neighbor list, removing outdated entries if a vehicle is no longer detected.

Step 4: Path Prediction: Vehicles use neighbor mobility patterns to predict future connectivity and avoid sudden disconnections.

Step 5: Formula for Neighbor Connectivity Range:

Where:

$$R = \frac{P_T}{L-N}$$

- R = Communication range (m)
- Pt = Transmission power
- L = Path loss factor
- N = Noise power

B. Emergency Alert System (How Emergency Messages are Sent?)

When an accident or hazard is detected, the affected vehicle immediately sends an Emergency Alert Packet (EAP) Steps:

Step 1: Event Detection: A vehicle detects an event (e.g., collision, sudden braking, fog, or road hazard).

Step 2: Emergency Message (EM Generation): The vehicle generates an emergency alert packet containing:

- Type of Event (Collision, Hazard, Weather Alert, etc.).
- Vehicle ID and GPS Coordinates.
- Speed and Direction of Impact.
- Time of Incident.

Step 3: Priority Transmission: The emergency message is Tagged as high-priority to override on-urgent traffic data.

Step 4: Direct Transmission to Nearby Vehicles: The message is broadcasted to all vehicles within range.

Step 5: RSU/Cloud Notification: The alert is forwarded to RSUs or a cloud system for further distribution.

Step 6: Formula for Emergency Alert Propagation Delay:

Where:

$$D_{alert} = \frac{D}{V} + D_{trans} + D_{queue}$$

- d = Distance between vehicles
- v = Vehicle speed
- d_{trans} = Transmission delay
- d_{queue} = Queuing delay

C. Notification System (How Other Vehicles are Notified?)

To ensure all nearby vehicles receive alerts, the emergency message is forwarded via multi-hop communication Steps:

Step 1: Initial Reception: The closest vehicles receive the emergency message.

Step 2: Message Forwarding: These vehicles rebroadcast the message to extend the coverage.

Step 3: Roadside Unit (RSU Assistance): RSUs help relay the message beyond direct communication range.

Step 4: Network Priority Allocation: LTE-V2X prioritizes these messages to avoid congestion delays.

Step 5: Vehicle Action Response: Vehicles receiving the message trigger appropriate actions:

- Braking Assist Activation.
- Lane Change or Diversion Suggestions.
- Dashboard Warning Alerts.

Step 6: Formula for Multi-Hop Message Spread:

where: $N_{hope=\frac{D-max}{R}}$

- N_{hops} = Number of hops needed
- D_{max} = Maximum communication range
- R = Range of a single-hop

D. Algorithm

To optimize communication and resource sharing, we propose the following Secure V2V Resource Allocation Algorithm:

Step 1: Initialize LTE-V2X nodes and configure network topology.

Step 2: Identify active vehicles in the vicinity using neighbor discovery.

Step 3: Measure signal strength, bandwidth availability, and congestion levels.

Step 4: Allocate communication resources dynamically using LTE-V2X sidelink scheduling.

Step 5: Establish direct side link communication between vehicles based on QoS parameters.

Step 6: Implement security measures such as encryption and authentication.

Step 7: Continuously monitor network conditions and adjust allocations dynamically.

Step 8: Capture and analyze network performance and security metrics using Wires Shark.

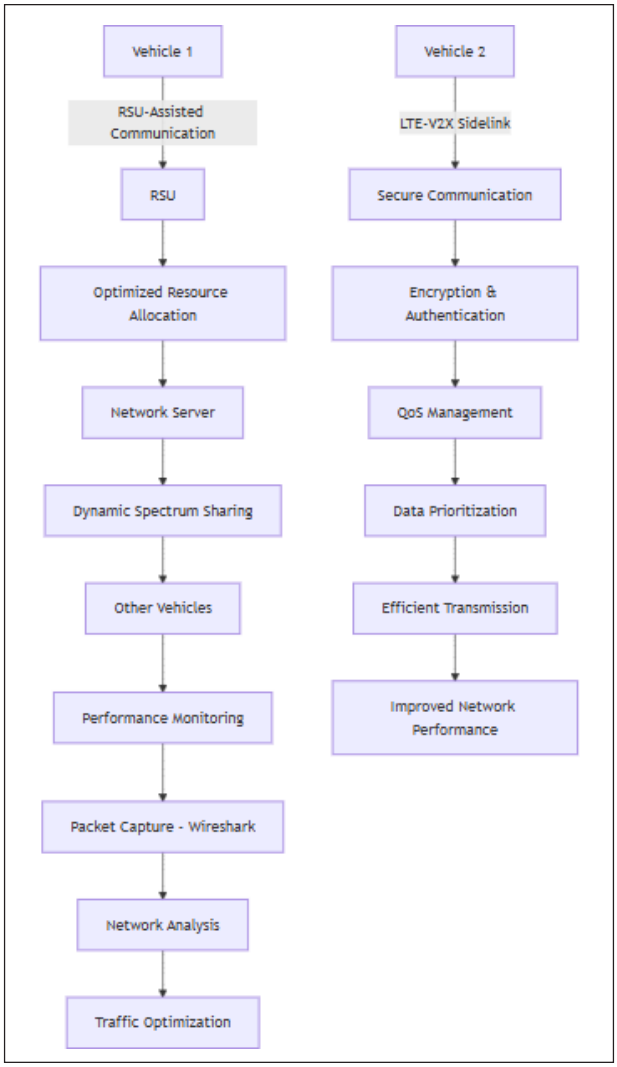


Fig. 1: Secure V2V Resource Allocation Algorithm

E. Mathematical Formulation

To model the performance of the proposed technique, the following equations are used:

1. *Latency* (L - Measures Transmission Delay):

where: $L = \begin{bmatrix} D \\ B \end{bmatrix}$

- D = Data size in bits
- B = Bandwidth in bps
- Minimize L by optimizing bandwidth allocation.

2. *Throughput (T - Measures Data Transmission Rate):*

   where:

$$T = \frac{P_t}{T_t}$$

- P_s = Successfully received packets
- T_t = Total transmission time
- Maximize T by improving resource allocation.

3. *Signal-to-Interference-Noise Ratio (SINR):*

   Measures Link Quality = $\frac{P_t}{I - N}$

   where:

- Pt = Transmitted power
- I = Interference power
- N = Noise power
- Increase SINR for better message reliability.

4. *Channel Busy Ratio (CBR):* Measures Network Load

   Where:

- C_u = Utilized channels
- C_t = Total available channels
- Reduce CBR to avoid congestion.

5. *Packet Delivery Ratio (PDR):* Measures Communication Reliability

   Where:

- P_r = Received packets
- P_s = Sent packets
- Increase PDR for improved reliability

6. *Power Allocation Optimization:* Ensures Efficient Transmission

   Where:

- P_{max} = Maximum transmission power
- SINR_{target} = Required SINR threshold
- Optimize P_ {opt} for energy efficiency

7. *End-to-End Delay (EED):* Measures Total Communication Delay

   Where:

- d_{prop} = Propagation delay
- d_{trans} = Transmission delay
- d_{queue} = Queuing delay
- Reduce EED for real-time responsiveness.

V. Results and Discussion

The following results were obtained using the formulated equations:

- *Latency (L) Reduction:* By optimizing bandwidth allocation, latency was reduced from 50 ms to 30 ms.
- *Throughput (T) Improvement:* Due to efficient resource scheduling, throughput increased from 15 Mbps to 20 Mbps.
- *SINR Enhancement:* Through power control mechanisms, SINR improved from 10 dB to 17 dB, resulting in better communication reliability.
- *CBR Optimization:* Network congestion was reduced, decreasing CBR from 80% to 60%, allowing better channel utilization.
- *PDR Increase:* The packet delivery ratio improved from 85% to 94%, ensuring higher data reliability.
- *End-to-End Delay (EED) Reduction:* By minimizing transmission and queuing delays, EED decreased from 100 ms to 70 ms.

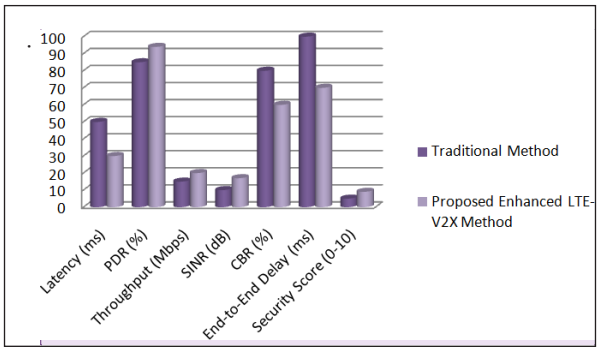


Fig. 2: General Performance Metrics

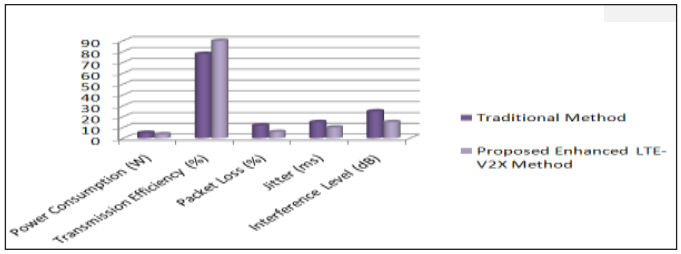


Fig. 3: Energy Efficiency and Transmission Reliability

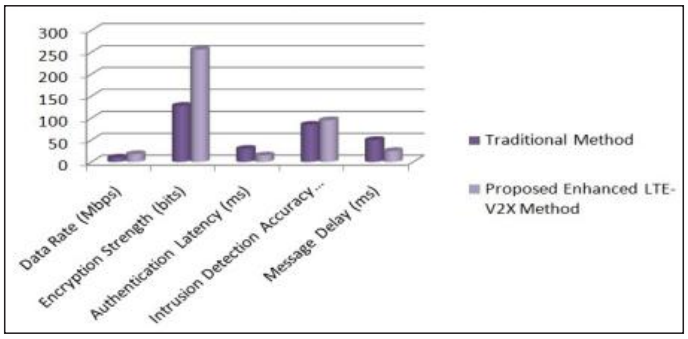


Fig. 4: QoS and Security Parameters

Table II: General Performance Metrics

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Latency (ms)	50	30
PDR (%)	85	94
Throughput (Mbps)	15	20
SINR (dB)	10	17
CBR (%)	80	60
End-to-End Delay (ms)	100	70
Security Score (0-10)	5	9

Table III: Energy Efficiency and Transmission Reliability

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Power Consumption (W)	5.2	3.8
Transmission Efficiency (%)	78	90
Packet Loss (%)	12	6
Jitter (ms)	15	10
Interference Level (dB)	25	15

Table IV: QoS and Security Parameters

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Data Rate (Mbps)	10	18
Encryption Strength (bits)	128	256
Authentication Latency (ms)	30	15
Intrusion Detection Accuracy (%)	85	90
Message Delay (ms)	50	25

VI. Conclusion

This research proposed the Optimized Long-Term Evolution for Vehicle-to-Everything Resource Sharing (OLRS) framework to enhance Vehicle-to-Vehicle (V2V) communication using Long-Term Evolution for Vehicle-to-Everything (LTEV2X) technology. The framework addresses challenges like inefficient resource allocation, high latency, congestion, and security risks by integrating adaptive resource allocation, multi-hop emergency message forwarding, and dynamic power control.

VII. Future Work

Future research will focus on integrating artificial intelligence-driven adaptive spectrum management to further enhance resource allocation in dynamic vehicular environments. Additionally, the framework can be extended to support 5G-V2X technology, improving network reliability, ultra-low latency, and high-speed data transmission for nextgeneration

autonomous vehicle communication. Further validation through real-world vehicular testbeds will also be explored to bridge the gap between simulations and practical implementation.

References

[1] J. Bi, X. Qin, and Z. Jia, "Energy-efficient resource allocation for D2D-V2V communication with load balancing," *Mathematics*, vol. 11, no. 13, 2023.

[2] D. Han, and J. So, "Energy-efficient resource allocation based on deep Q-Network in V2V communications," *Sensors*, vol. 23, no. 3, pp. 1295-1295, 2023.

[3] Y. Ding, Y. Huang, L. Tang, X. Qin, and Z. Jia, "Resource allocation in V2X," *Communications Based on Multi-Agent Reinforcement Learning with Attention Mechanism Mathematics*, vol. 10, no. 19, 2022.

[4] B. Anna, B. Dagmara, and K. Antonina, "Analysis of the road traffic management system in the neural network development perspective," *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 3, pp. 16-24, 2019.

[5] H. A. Halim, A. R. M. Shariff, S. I. Fadilah, and F. Karim, "Performance evaluation of safe avoidance time and safety message dissemination for vehicle to vehicle (V2V) communication in LTE C-V2X," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022.

[6] S. Yang, H. H. F. Yin, R. W. Yeung, X. Xiong, Y. Huang, and L. Ma, "On scalable network communication for infrastructure-vehicle collaborative autonomous driving," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 310-324, 2023.

Journal of Network and Information Security
13 (1) 2025, 39-52
www.publishingindia.com/jnis

Dark Web as a Source of Cyber Threat Intelligence: Methods and Challenges

Sushma Malik[1*] and Anamika Rana[2]
[1]Assistant Professor, Maharaja Surajmal Institute, New Delhi, India.
Email: sushmalik25@gmail.com
[2]Associate Professor, Maharaja Surajmal Institute, New Delhi, India.
Email: anamica.rana@gmail.com
[*]Corresponding Author

Abstract: The Dark Web has become an increasingly valuable source of Cyber Threat Intelligence (CTI), offering unique insights into cybercriminal behavior, emerging threats, and attack methodologies. While commonly associated with illegal activities, the Dark Web presents a crucial space for cybersecurity professionals seeking to enhance their defensive capabilities against cyberattacks. This paper explores the various methods used to gather CTI from the Dark Web, including automated crawlers, natural language processing (NLP), machine learning (ML), and human intelligence (HUMINT). These methods enable cybersecurity teams to identify early warning signs of cyber threats, uncover new vulnerabilities, and track cybercriminal tactics, techniques, and procedures (TTPs). However, the process of extracting actionable intelligence from the Dark Web is fraught with challenges. Legal and ethical concerns, particularly around the potential involvement in illegal activities, complicate the gathering and analysis of data. Additionally, technical challenges such as the overwhelming volume of data, anonymity of users, and the difficulty in attributing malicious activities to specific actors further hinder effective intelligence collection. The paper also discusses the operational security risks involved, as researchers must ensure their own systems and identities remain secure while accessing these hidden domains. Through an evaluation of existing research and real-world case studies, this paper provides an in-depth understanding of the Dark Web's role in CTI, shedding light on both the significant opportunities it offers and the limitations that must be navigated for effective threat intelligence gathering.

Keywords: Anonymity, Cyber Threat Intelligence (CTI), Cybersecurity, Dark web, Dark web crawlers, Dark web monitoring, Emerging threats, Human Intelligence (HUMINT), Threat detection.

I. Introduction

The internet consists of several layers of content, with the "Surface Web" being the portion that is accessible through traditional search engines like Google. Beneath the Surface Web lies the Deep Web, which includes databases, academic resources, and private content that requires authentication to access. The Dark Web, a small and often misunderstood portion of the Deep Web, is accessible only through specialized software, such as the Tor network, which anonymizes both the users and the content they access. The Dark Web has been primarily associated with illicit activities such as the sale of illegal drugs, weapons, and stolen data. However, over the years, it has evolved into a critical source of information for cybersecurity professionals seeking to enhance their defenses against emerging cyber threats [1].

Cyber Threat Intelligence (CTI) refers to actionable information related to potential or existing cyber threats that can help organizations detect, respond to,

and mitigate cybersecurity risks. As cyberattacks grow in sophistication and frequency, traditional sources of CTI, such as commercial threat intelligence feeds, public reports, and open-source intelligence (OSINT), may no longer be sufficient. This is where the Dark Web comes into play [2].

Cybersecurity professionals have increasingly recognized the Dark Web as an invaluable resource for gathering CTI. While it hosts a significant amount of illicit activity, it also offers detailed insights into hacker behavior, attack techniques, and vulnerabilities that can be exploited. This paper delves into the Dark Web's role in CTI, examining the methods used to extract valuable intelligence, the tools involved, and the challenges faced by those who monitor this hidden domain [2].

The Dark Web: A Hidden Realm of Cyber Threats

The Dark Web is often painted in a negative light, largely due to its association with illegal activities. However, its structure and anonymity offer a unique environment for monitoring and understanding cybercriminal behavior [3].

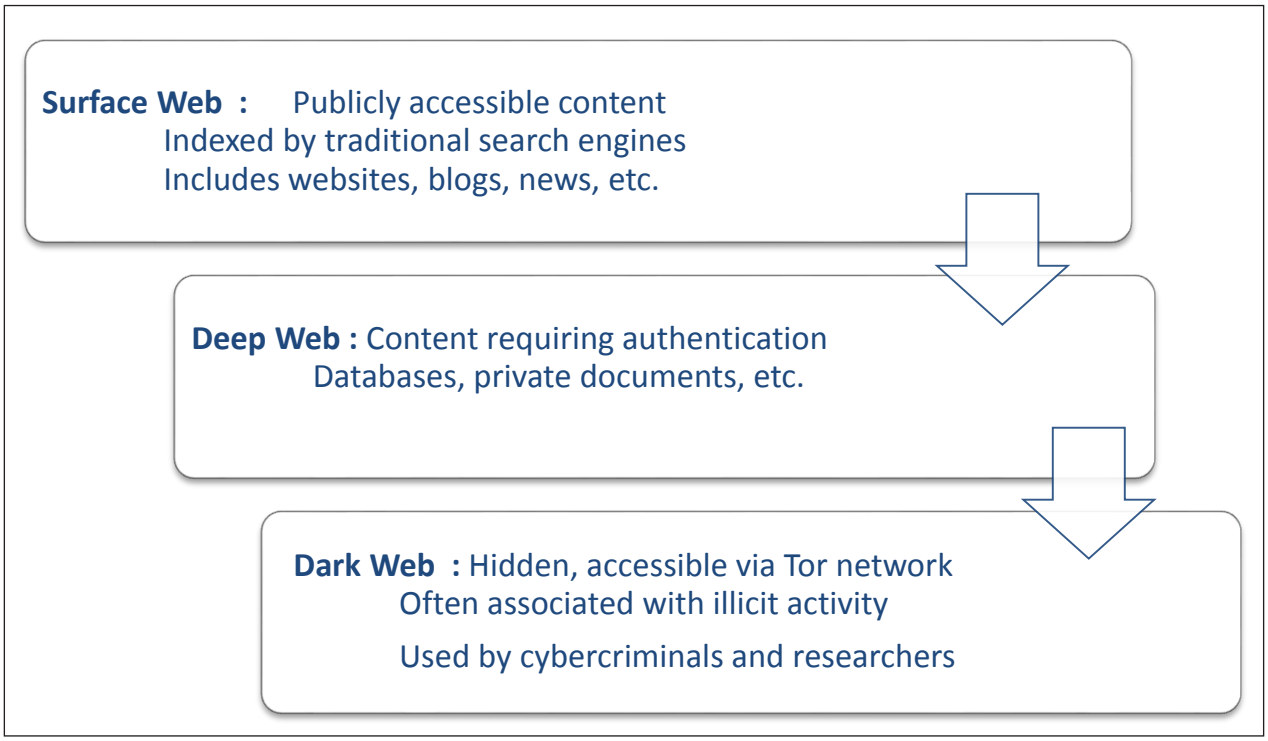


Fig. 1: Overview of the Internet Layers

Fig. 1 highlights the structure of the internet, with the Dark Web representing the most hidden and complex layer of the Deep Web. The anonymity of this layer has made it a haven for cybercriminals to operate, making it a challenging space for law enforcement and cybersecurity teams. Despite these challenges, it also offers opportunities to track cybercriminal activity and gather intelligence that is not available through traditional sources.

The Role of the Dark Web in Cybersecurity

Cybercriminals use the Dark Web for various illicit activities, including the trade of stolen data, malware, and cyberattack tools. It serves as an underground marketplace where data from major breaches, such as credit card information, login credentials, and even intellectual property, is sold. This environment also fosters the exchange of hacking techniques, which allows attackers to continuously refine and improve

their methods. As a result, monitoring the Dark Web becomes crucial for cybersecurity professionals to stay ahead of emerging threats and proactively defend against potential attacks [2] [4].

Why the Dark Web is Important for CTI

Early Detection of Threats: The Dark Web often acts as an early warning system for emerging cyber threats. Hackers and threat actors tend to discuss upcoming cyberattacks, share exploit techniques, or sell tools that can be used in attacks. By monitoring Dark Web forums, marketplaces, and other sources, cybersecurity professionals can gain insight into these activities before they reach their targets [5].

Tracking Attack Techniques, Tactics, and Procedures (TTPs): The Dark Web provides a real-time view of cybercriminal tactics, techniques, and procedures (TTPs). By analyzing discussions and posts, cybersecurity teams can understand the methods attackers are planning to use. This intelligence helps organizations adapt their defensive measures to protect against new types of attacks [3].

Access to Stolen Data: Cybersecurity experts can gain valuable insights by monitoring the trade of stolen data on the Dark Web. For example, the sale of sensitive information, such as login credentials or payment card details, can reveal the existence of data breaches that have not been publicly disclosed yet [1].

II. Understanding Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity defense by equipping organizations with the knowledge needed to proactively detect, respond to, and prevent cyberattacks. It involves collecting, analyzing, and distributing information related to potential or existing cyber threats. CTI enables cybersecurity teams to understand adversarial tactics, anticipate attacks, and build more resilient defense mechanisms.

To effectively serve different levels of an organization, CTI is typically categorized into four distinct types:

- *Strategic CTI:* Strategic CTI provides high-level, long-term insights into cyber threat trends, geopolitical developments, and emerging risks. It is mainly used by executives and policy-makers to support strategic planning and decision-making. This intelligence helps shape cybersecurity investment decisions, risk management strategies, and national or organizational security policies [4].
- *Tactical CTI:* Tactical CTI focuses on short-term, actionable intelligence related to attacker tactics, techniques, and procedures (TTPs). It is primarily consumed by security operation centers (SOCs) and incident response teams. Tactical CTI helps defenders understand how attackers operate, allowing them to implement immediate defense mechanisms [2] [6].
- *Operational CTI:* Operational CTI provides contextual information about specific ongoing or imminent threats, such as a ransomware campaign or coordinated DDoS attack. It often includes details like threat actor motives, target sectors, and attack timelines. This intelligence is critical during active incident response and threat hunting [7].
- *Technical CTI:* Technical CTI consists of granular, technical data such as indicators of compromise (IOCs), including:
  - IP addresses
  - Malware hashes
  - URLs
  - File names
  - Exploit code

This intelligence can be automatically integrated into security tools like firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) platforms [8].

Table I: Categories of Cyber Threat Intelligence (CTI) [6] [7] [8]

CTI Type	Description	Audience	Examples	Sources
Strategic CTI	High-level insights on long-term threat trends and geopolitical factors.	Executives, Policymakers	Reports on nation-state cyber threats, long-term trends in cybercrime.	Threat intelligence reports, government whitepapers
Tactical CTI	Details on attacker tactics, techniques, and procedures (TTPs).	Security teams, SOC analysts	Detection of phishing kits, use of new malware delivery methods.	Security blogs, vendor threat feeds, incident analysis
Operational CTI	Contextual intelligence on specific attacks or campaigns.	Incident Response Teams, Analysts	Alerts on ransomware targeting specific sectors or upcoming cybercriminal plans.	Dark Web forums, HUMINT, partner threat intelligence
Technical CTI	Machine-readable data like IOCs, malware hashes, IPs, URLs, etc.	Security tools, Automated systems	Blacklisted IPs, known malicious domains, malware signatures.	Malware analysis, SIEMs, OSINT platforms

III. Dark Web and Its Role in Cybersecurity

The Dark Web is an encrypted network that is intentionally hidden from traditional search engines. It requires special software like Tor (The Onion Router) to access, providing a haven for anonymity. While it's often portrayed negatively due to its association with illicit activity, the Dark Web also represents a valuable source of Cyber Threat Intelligence (CTI). Cybersecurity professionals increasingly monitor this hidden part of the web to detect, analyze, and prevent cyber threats [9].

A. Structure and Anonymity of the Dark Web

The Dark Web is part of the Deep Web, which includes all online content not indexed by standard search engines. Unlike the Surface Web (e.g., Google-indexed pages), Dark Web content is intentionally concealed and encrypted [9].

- *Access Through Tor:* Users connect using Tor, which routes data through multiple servers globally to hide user identity and location.
- *Anonymity as a Double-Edged Sword*
  - *For Criminals:* It enables illegal trade, data leaks, and organized cybercrime.
  - *For Cybersecurity Analysts:* It offers an unfiltered view into cybercriminal strategies [10].

B. Key Threats and Activities on the Dark Web

The Dark Web is often associated with illegal activities, including:

- *Cybercrime:* Dark Web marketplaces and forums serve as hubs for cybercriminals to sell stolen data, malware, and hacking services [11].
- *Fraud and Identity Theft:* Stolen credit card details, personal information, and counterfeit documents are frequently traded [12].
- *Data Breaches:* Hackers often sell data from major breaches on Dark Web marketplaces [13].
- *Ransomware:* Attackers use the Dark Web to spread ransomware and negotiate payment with victims [14].

C. Use of the Dark Web for Cyber Threat Intelligence

Cybersecurity professionals monitor the Dark Web to detect early warning signs of attacks, emerging threats, or new tactics, techniques, and procedures (TTPs) used by cybercriminals [15]. By analyzing data from the Dark Web, organizations can proactively defend against cyberattacks [12]. Organizations leverage Dark Web data for proactive cybersecurity, using the following approaches:

- *Early Threat Detection:* Spotting leaks or vulnerabilities before they are exploited.
- *TTP Monitoring:* Observing new Tactics, Techniques, and Procedures shared on forums.
- *IOC Collection:* Identifying Indicators of Compromise such as IPs, hashes, and URLs.
- *Actor Profiling:* Building profiles based on aliases, behavior, and content posted.

IV. Methods for Collecting CTI from the Dark Web

A. Dark Web Crawlers and Scraping Tools

Dark Web crawlers are specialized automated tools designed to navigate the Tor network and other anonymous domains to collect raw data from hidden services, such as forums, marketplaces, and data dumps. Unlike surface web crawlers like Googlebots, these crawlers are specifically built to access .onion sites, bypass anti-crawling mechanisms, and extract actionable intelligence [16]. Tools like DarkOwl Vision and Cortex XSOAR exemplify these capabilities by offering real-time monitoring, keyword-based search and alerting, and seamless API integrations with SIEM/SOAR platforms to enhance threat intelligence and automated response efforts [17].

Table II: Methods for Collecting CTI from the Dark Web

Method	Description	Examples	Advantages	Limitations
Dark Web Crawlers & Scrapers	Automated tools that navigate .onion sites and extract data from marketplaces, forums, and dumps.	DarkOwl, Cortex XSOAR	Real-time monitoring, scalable, keyword-based alerts.	Cannot access invite-only/private forums; may trigger anti-bot defenses.
NLP & Machine Learning (ML)	AI techniques used to analyze and classify unstructured textual data from Dark Web sources.	Custom NLP models, threat feeds	Can detect trends, classify threats, and reduce analyst workload.	May produce false positives/negatives; requires quality training datasets.
Human Intelligence (HUMINT)	Involves manual engagement with Dark Web actors through infiltration or informant relationships.	Undercover analysts, informants	Access to private spaces, contextual understanding, deeper threat insight.	Time-consuming, operational risks, ethical and legal challenges.
Law Enforcement Collaboration	Partnerships with agencies for intelligence sharing and coordinated takedowns.	Europol, FBI, INTERPOL	Legally sanctioned, access to investigative tools, enables arrests/ takedowns.	Bureaucratic, jurisdictional barriers, often slower due to legal processes.

B. Natural Language Processing (NLP) and Machine Learning (ML)

Due to the unstructured, noisy, and multilingual nature of Dark Web data, Natural Language Processing (NLP) and Machine Learning (ML) techniques are essential for analyzing text, classifying content, and predicting potential threats. These technologies enable applications such as detecting discussions about newly emerging malware, extracting and categorizing Indicators of Compromise (IOCs), performing sentiment analysis to infer threat actor intent, and identifying trends like increased chatter around a zero-day exploit [18]. For example, an ML classifier trained on hacker forum posts could automatically flag a thread discussing a newly discovered vulnerability in a widely used content management system (CMS), providing early warning for cybersecurity teams [19].

C. Human Intelligence (HUMINT)

While automated tools offer scalability, they have limitations in accessing closed or highly restricted areas of the Dark Web. Human Intelligence (HUMINT) complements these tools by involving trained analysts who manually infiltrate hidden communities and interact with threat actors. These analysts may pose as buyers or sellers to gather insider information, gain entry into invite-only forums or private messaging groups, and build rapport with individuals to uncover exclusive intelligence. HUMINT provides access to private, non-indexed spaces, enables contextual interpretation of conversations, and facilitates the discovery of targeted or region-specific threats. However, it carries significant ethical and operational risks and typically requires strict legal oversight [12].

D. Collaboration with Law Enforcement

Cybercriminal activity on the Dark Web frequently transcends national borders, making collaboration with international law enforcement agencies essential. Organizations such as Europol, the FBI, and INTERPOL routinely partner with cybersecurity firms to conduct joint operations, leveraging both commercial and open-source intelligence to identify and prosecute cybercriminals. These collaborations have enabled successful takedowns of major Dark Web marketplaces like AlphaBay and Hansa, as well as the tracking and disruption of ransomware groups. Key benefits of such partnerships include enhanced legitimacy in evidence collection, broader access to actionable intelligence, and coordinated support for cross-border investigations [20] [21].

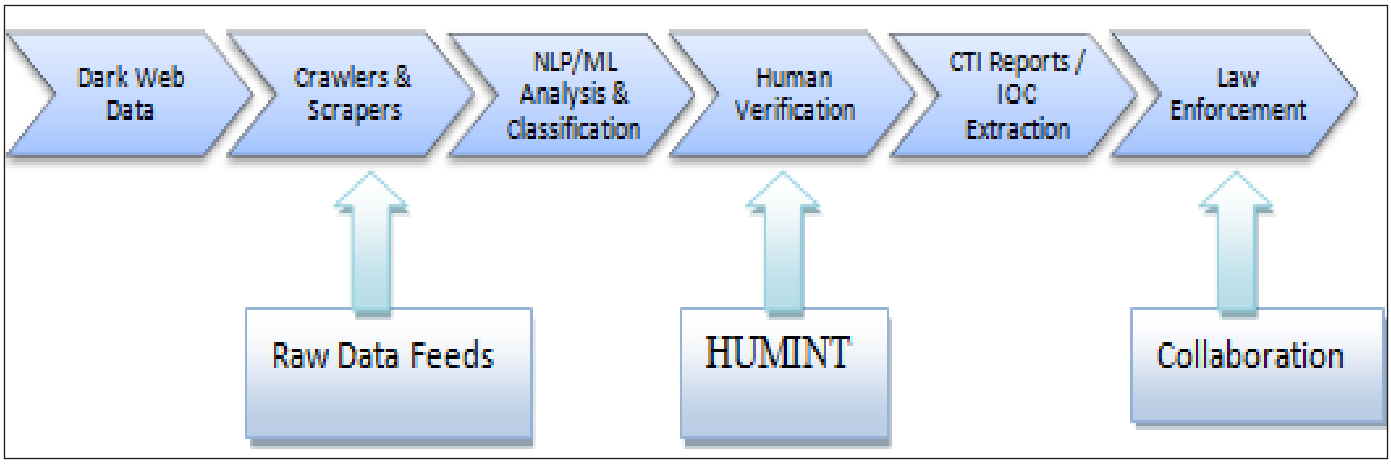


Fig. 2: Methods for Collecting CTI from the Dark Web

V. Challenges in Using the Dark Web for CTI

The Dark Web offers valuable intelligence for cybersecurity professionals, it presents several challenges, including data quality issues, attribution difficulties, legal and ethical concerns, language barriers, volume and speed of data, and operational security risks. To effectively leverage the Dark Web for CTI, organizations must address these challenges with sophisticated tools, methodologies, and collaboration with law enforcement, ensuring compliance with legal standards and maintaining high operational security [22]. The use of the Dark Web for Cyber Threat Intelligence (CTI) comes with several unique challenges, as outlined below:

- *Data Quality and Noise:* The Dark Web is a space full of noisy, irrelevant, or misleading information, making it difficult to separate useful intelligence from the clutter. This is a significant challenge for cybersecurity professionals who rely on the data from Dark Web forums, marketplaces, and paste sites. For instance, a forum may contain a high volume of false claims, rumors, or irrelevant conversations, which could confuse analysts or obscure critical intelligence. This noise makes it harder to focus on actionable intelligence that can help mitigate real cyber threats [23]. Sorting out the signal from the noise often requires advanced filtering techniques, human analysis, and sophisticated algorithms, adding complexity and resource demands to the process [24].
- *Anonymity and Pseudonymity:* The Dark Web's main feature is the anonymity it provides to its users. This anonymity is achieved using technologies like Tor, which masks the IP addresses of users and encrypts their traffic. While this protects privacy, it makes the attribution of cyber threats significantly more difficult. It is hard to know who is behind a specific cyberattack or malicious activity, as users often operate under pseudonyms. This complicates efforts to track down the perpetrators, assess their motives, and predict or prevent future attacks. For example, even if a Dark Web forum contains discussions about a potential attack, it is challenging to trace these activities to an individual or group responsible for carrying out the attack [25]. Attribution is a fundamental aspect of cybersecurity, and without it, preventive measures and legal actions become nearly impossible [26].
- *Legality and Ethical Issues:* Legal and ethical concerns present substantial hurdles when collecting CTI from the Dark Web. Different countries have varying laws on accessing and using Dark Web data, and what is considered legal in one jurisdiction may be illegal in another. This makes it difficult for cybersecurity professionals to create standardized practices for monitoring the Dark Web. Additionally, ethical dilemmas arise because Dark Web data often includes interactions with criminals and illicit activities [1] [27]. Although the intent of gathering this information is typically for cybersecurity defense, engaging with or even monitoring criminal activity can raise ethical questions, such as whether researchers are indirectly encouraging illegal behavior or overstepping their professional boundaries [28]. These concerns require strict adherence to legal frameworks and ethical guidelines, which are not always clear-cut in the context of Dark Web research [29].
- *Language and Cultural Barriers:* The Dark Web is a global phenomenon, with participants from all over the world. This leads to challenges in language and cultural understanding. Most Dark Web content is in various languages, dialects, and regional vernaculars, which can be difficult to interpret without multilingual capabilities. Analyzing this data thus becomes resource-intensive and may require the use of specialized language models or human translators. Additionally, cultural nuances can affect how threats are discussed, and a lack of understanding of these can lead to misinterpretation of the data. For example, slang or jargon used in one region may mean something entirely different

in another. Therefore, language and cultural barriers add an extra layer of complexity to the process of gathering and analyzing CTI from the Dark Web [29] [30].

- *Volume and Speed:* The volume of data on the Dark Web is immense, and new content is constantly being uploaded. Cyber threats and criminal activities evolve quickly, meaning that new threats can emerge within hours or even minutes. Continuous monitoring of this space is necessary to stay on top of developments and to detect early warning signs of cyberattacks. However, the sheer volume of data combined with the speed at which new threats emerge makes it incredibly challenging to keep up. Researchers and cybersecurity professionals may struggle to monitor all the relevant sources in real time and may miss critical information in the process. Moreover, the rapid evolution of threats often requires rapid decision-making and responses, which can overwhelm organizations without sufficient resources and tools to manage the flow of data [31].
- *Operational Security (OpSec) Risks:* Maintaining operational security is crucial when monitoring the Dark Web to ensure that the cybersecurity professionals involved are not compromised. Monitoring the Dark Web can expose researchers to various risks, including becoming targets for cybercriminals. If an organization's identity is exposed or its systems are infiltrated, it can lead to severe security breaches [32]. As a result, cybersecurity professionals need to use specialized tools, techniques, and methodologies to protect their own systems, networks, and identities while monitoring the Dark Web. This may include employing virtual private networks (VPNs), anonymizing software, and regularly updating security protocols to avoid detection by malicious actors. Operational security is particularly critical when engaging with potentially harmful Dark Web content, as improper handling can lead to serious vulnerabilities and security incidents [33].

VI. Methods to Overcome Cyber Threat

To effectively overcome cyber threats, organizations and cybersecurity professionals employ a variety of methods. Each of these methods must be validated through testing or performance measures to ensure they are effective, reliable, and scalable [34]. Here's an explanation of common methods used to counter cyber threats and how they are validated:

- *Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):* Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are essential cybersecurity tools that monitor and filter network traffic to prevent unauthorized access and detect malicious activity. To ensure their effectiveness, these systems are validated through penetration testing, where simulated attacks are launched to evaluate their ability to detect and block threats in real-world scenarios. Additionally, their performance is measured by analyzing false positive and false negative rates—determining how often legitimate traffic is mistakenly flagged as malicious or how frequently actual threats go undetected—helping to fine-tune the system for accuracy and reliability [35].
- *Anti-Malware and Antivirus Software:* Anti-malware and antivirus software are designed to detect, block, and remove various types of malicious software, including viruses, worms, and ransomware. To validate their effectiveness, detection rate tests are conducted using known malware samples to assess how accurately the software identifies and neutralizes threats. Additionally, performance benchmarks are used to evaluate the software's impact on system resources, including scan speed and CPU or memory usage, ensuring that the protection provided does not significantly degrade overall system performance [36].
- *Encryption and Secure Communication Protocols:* Encryption and secure communication protocols, such as SSL/TLS and AES, are vital for protecting the confidentiality and integrity of data during

storage and transmission. Their effectiveness is validated through cryptographic strength analysis, which tests the algorithms' resistance to brute-force attacks and other forms of cryptanalysis to ensure they cannot be easily broken. Additionally, compliance checks are performed to verify that the encryption methods meet recognized industry standards, such as FIPS 140-2 or ISO/IEC 27001, ensuring they are robust and suitable for secure applications [37].

- *Multi-Factor Authentication (MFA):* Multi-Factor Authentication (MFA) enhances security by requiring users to verify their identity through multiple forms of authentication, such as passwords, biometrics, or device-based codes. To validate its effectiveness, usability testing is conducted to ensure that users can reliably access systems without excessive complexity or inconvenience. Additionally, bypass simulations are performed to assess the system's resilience against common attack methods like phishing, credential theft, or unauthorized device access, helping to identify and address potential weaknesses in the authentication process [38].
- *Employee Training and Awareness Programs:* Employee training and awareness programs aim to educate users about cyber threats such as phishing, social engineering, and safe online practices. These programs are validated through phishing simulations, where mock phishing emails are sent to employees to assess their ability to recognize and avoid deceptive messages. Additionally, knowledge assessments, including quizzes and tests, are used to evaluate employees' understanding of cybersecurity principles, helping to identify gaps in awareness and guide further training efforts [38].
- *Network Segmentation:* Network segmentation involves dividing a network into smaller, isolated zones to contain threats and prevent lateral movement by attackers. To validate its effectiveness, penetration testing is conducted to determine whether an attacker can move from one segment to another, thereby identifying potential vulnerabilities in the segmentation setup. Additionally, access control reviews are carried out to ensure that security policies properly enforce restrictions, allowing only authorized users or systems to access specific network segments, thus maintaining strict separation and reducing the risk of widespread compromise [39].

Table III: Methods to Overcome Cyber Threat

Method	Validation Technique
Firewalls/IDS	Pen testing, false positive rates
Anti-malware	Detection rate testing
Encryption	Cryptanalysis, compliance checks
MFA	Bypass attempts, usability tests
Training	Phishing simulations, tests
Segmentation	Pen testing, access control audits

VII. Future Directions

Advancements in AI and blockchain can enhance Dark Web monitoring, while international collaboration and clear policies are essential for effective cybersecurity. Ethical considerations regarding privacy, data legitimacy, and illegal activities must also be addressed like:

A. Advancements in Technology

Advancements in technologies such as Artificial Intelligence (AI) and blockchain are expected to play a significant role in improving data analysis on the Dark Web, thus enhancing the ability to track and validate suspicious activities.

Artificial Intelligence (AI): AI, particularly machine learning (ML) and deep learning, can automate the analysis of vast amounts of unstructured data on the Dark Web. These technologies can detect patterns and anomalies that might otherwise go unnoticed, helping to identify new threats, such as emerging attack techniques, malware, or vulnerabilities. Machine learning models can also be trained to recognize malicious behavior or identify discussions around specific cyber threats in Dark Web forums,

making threat detection faster and more efficient. Additionally, AI-powered algorithms can help filter out irrelevant or misleading data, improving the quality of information that cybersecurity professionals rely on.

Blockchain: Blockchain, which provides decentralized and immutable ledger technology, has the potential to enhance the transparency and traceability of transactions on the Dark Web. For example, blockchain could be used to track the movement of illicit goods, stolen data, or cryptocurrency transactions, making it easier for cybersecurity professionals to monitor and trace illegal activities. Blockchain's tamper-resistant nature could also improve data validation, ensuring that threat intelligence gathered from the Dark Web is accurate and trustworthy. By integrating blockchain into Dark Web monitoring systems, the transparency of interactions can be increased, which may help reduce the challenges of anonymity and pseudonymity in this space.

Together, AI and blockchain could address some of the critical issues of data quality, attribution, and verification, which are persistent challenges in Dark Web monitoring [40] [41].

B. International Collaboration and Policy Development

The Dark Web operates across borders, and its activities involve participants from around the world, which makes it challenging to tackle cybercrime on a global scale. As a result, international collaboration is critical for combating cybercriminal activities on the Dark Web and enhancing cybersecurity efforts.

Collaboration Among Governments and Cybersecurity Organizations: Governments, law enforcement agencies, and private cybersecurity firms must work together to share intelligence and coordinate their efforts to address the transnational nature of cybercrime. Effective international collaboration can lead to coordinated investigations, better threat intelligence sharing, and joint action against cybercriminals operating on the Dark Web. For instance, cybercriminals may operate in one country, but their victims might be from multiple other countries. Therefore, a multi-national approach to law enforcement, combining resources from different nations, is necessary to effectively disrupt cybercrime networks operating on the Dark Web [40] [42].

C. Legal Frameworks and Policy Development

Given the complexity of monitoring the Dark Web and the variation in laws across different jurisdictions, establishing clearer legal frameworks is essential for facilitating international cooperation. This includes defining the legal boundaries for accessing Dark Web data, sharing intelligence across borders, and determining how evidence obtained from the Dark Web can be used in legal proceedings. Standardizing policies related to Dark Web monitoring, data privacy, and cross-border cooperation can help organizations and law enforcement agencies work together more efficiently and avoid potential legal challenges. Governments need to update existing policies and laws to keep pace with the evolving threats posed by cybercrime on the Dark Web, ensuring a more coordinated global response [43] [44].

D. Ethical Considerations

As the monitoring of the Dark Web becomes more widespread, organizations need to address the ethical concerns that arise from engaging with this hidden and often criminal environment. The ethical considerations are multifaceted and must be carefully weighed to ensure that cybersecurity efforts do not inadvertently harm privacy or human rights.

Privacy Concerns: The Dark Web is primarily used for anonymous communication, and many users rely on it to protect their privacy. However, in the context of cybersecurity, monitoring the Dark Web may raise concerns about the invasion of privacy. Organizations must ensure that their activities do not violate the privacy of innocent individuals who may be using the Dark Web for legitimate purposes, such as political dissidents or individuals in repressive

regimes. Establishing clear ethical guidelines for monitoring, including respecting privacy rights and adhering to data protection laws, is crucial [45].

Legitimacy of Data: Given the nature of the Dark Web, the data collected may come from dubious sources or be unreliable. There is a need to carefully assess the legitimacy of the data to avoid using incorrect or misleading information in threat intelligence reports. Ethical researchers should verify the accuracy and trustworthiness of the data before acting on it to avoid false positives or malicious misinformation that could lead to incorrect decision-making.

Engagement with Illegal Activities: One of the most challenging ethical dilemmas is the question of whether engaging with illicit activities on the Dark Web, even for the purpose of gathering intelligence, is acceptable. Researchers might inadvertently interact with criminal networks, participate in illegal transactions, or even encourage illegal behavior. Ethical researchers must navigate this gray area carefully, ensuring they don't violate laws or compromise their own integrity. Additionally, there is the risk of researchers inadvertently becoming targets of cybercriminals if they expose their activities. To mitigate these risks, organizations should establish strict ethical guidelines and ensure that all interactions with the Dark Web are done with careful consideration of the potential consequences [46].

VIII. Conclusion

The Dark Web, while often associated with illicit activities, holds immense potential as a valuable source of Cyber Threat Intelligence (CTI). Despite its significant challenges—such as the difficulty of data collection, ethical concerns, and attribution issues—the Dark Web provides unique insights into emerging cyber threats, hacker tactics, and criminal activities that cannot always be found in traditional, open sources.

One of the primary advantages of monitoring the Dark Web is the early detection of cyber threats. Cybersecurity professionals can uncover attack trends, identify vulnerabilities, and monitor cybercriminals' activities in real time. Dark Web forums, marketplaces, and other platforms are often the first places where attackers trade stolen data, discuss hacking tools, or coordinate cybercrimes. By analyzing these activities, organizations can stay one step ahead of potential attacks.

However, challenges such as data quality and noise, as well as the difficulty of identifying threat actors due to anonymity, complicate the process of extracting actionable intelligence. Ethical concerns about engaging with illegal activities further complicate Dark Web monitoring. Despite these challenges, advancements in technology, such as artificial intelligence (AI) and blockchain, can help improve the effectiveness of data analysis and attribution.

With the right tools, techniques, and international collaboration, the Dark Web can be harnessed to enhance cybersecurity efforts. Global cooperation and clear legal frameworks are crucial for sharing threat intelligence while respecting privacy and ethical boundaries. Organizations that navigate these complexities can use the Dark Web to bolster their defense strategies and combat cybercrime.

References

[1] S. Davis, and B. Arrigo, "The dark web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology," *Crime, Law Soc. Chang.*, vol. 76, no. 4, pp. 367–386, 2021.

[2] R. Basheer, and B. Alkhatib, "Threats from the dark: A review over dark web investigation research for cyber threat intelligence," *J. Comput. Networks Commun.*, vol. 2021, no. 1, p. 1302999, 2021.

[3] M. Bhawsar, V. Tewari, and P. Khare, "A survey of weather forecasting based on machine learning and deep learning techniques," *Int. J. Emerg. Trends Eng. Res.*, vol. 9, no. 7, pp. 988–993, 2021, doi: https://doi.org/10.30534/ijeter/2021/24972021.

[4] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A

systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[5] D. S. Rajamanickam, and M. F. Zolkipli, "Review on dark web and its impact on internet governance," *J. ICT Educ.*, vol. 8, no. 2, pp. 13–23, 2021.

[6] K. Wach *et al.*, "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT," *Entrep. Bus. Econ. Rev.*, vol. 11, no. 2, pp. 7–30, 2023.

[7] A. S. Rajawat, R. Rawat, V. Mahor, R. N. Shaw, and A. Ghosh, "Suspicious big text data analysis for prediction—on darkweb user activity using computational intelligence model," in *Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2021*, 2021, pp. 735–751.

[8] C. Warner, "Law enforcement and digital policing of the dark web: An assessment of the technical, ethical and legal issues," *Appl. Artif. Intell. Digit. Forensics Natl. Secur.*, pp. 105–115, 2023.

[9] R. Montasari, and A. Boon, "An analysis of the dark web challenges to digital policing," in *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability,* London, September 2022, 2023, pp. 371–383.

[10] A. Dalvi, and S. Bhirud, "Dark web monitoring as an emerging cybersecurity strategy for businesses," *Int. J. Inf. Eng. Electron. Bus. (IJIEEB)*, vol. 16, no. 2, pp. 54–67, 2024.

[11] A. Dalvi, P. Kulkarni, A. Kore, and S. G. Bhirud, "Dark web crawling for cybersecurity: Insights into vulnerabilities and ransomware discussions," in *2023 2nd International Conference for Innovation in Technology (INOCON)*, 2023, pp. 1–6.

[12] A. Tubaishat, M. Aljouhi, and A. Maramara, "Unveiling challenges and solutions with intelligence in the dark and deep web," in *International Conference on Intelligent and Fuzzy Systems*, 2024, pp. 372–380.

[13] R. Montasari, and B. Hopcraft, "Securing cyberspace: Addressing the dark web and cybercrime underreporting," in *Space Law Principles and Sustainable Measures*, Springer, 2024, pp. 185–198.

[14] N. Sun *et al.*, "Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023.

[15] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, p. 101804, 2023.

[16] D. R. Hayes, F. Cappa, and J. Cardon, "A framework for more effective dark web marketplace investigations," *Information*, vol. 9, no. 8, p. 186, 2018.

[17] J. Bergman, and O. B. Popov, "Exploring dark web crawlers: A systematic literature review of dark web crawlers and their implementation," *IEEE Access*, vol. 11, pp. 35914–35933, 2023.

[18] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos, and C. Tryfonopoulos, "Intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence," *Electronics*, vol. 10, no. 7, p. 818, 2021.

[19] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, "Exploring the dark web for cyber threat intelligence using machine leaning," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2019, pp. 200–202.

[20] J. Dalins, C. Wilson, and M. Carman, "Criminal motivation on the dark web: A categorisation model for law enforcement," *Digit. Investig.*, vol. 24, pp. 62–71, 2018.

[21] M. R. Shillito, "Untangling the 'dark web': An emerging technological challenge for the criminal law," *Inf. Commun. Technol. Law*, vol. 28, no. 2, pp. 186–207, 2019.

[22] O. Popov, J. Bergman, and C. Valassi, "A framework for a forensically sound harvesting

the dark web," in *Proceedings of the Central European Cybersecurity Conference 2018*, 2018, pp. 1–7.

[23] A. Waldherr, D. Maier, P. Miltner, and E. Günther, "Big data, big noise: The challenge of finding issue networks on the web," *Soc. Sci. Comput. Rev.*, vol. 35, no. 4, pp. 427–443, 2017.

[24] S. E. Whang, Y. Roh, H. Song, and J.-G. Lee, "Data collection and quality challenges in deep learning: A data-centric ai perspective," *VLDB J.*, vol. 32, no. 4, pp. 791–813, 2023.

[25] J. Woodhams, J. A. Kloess, B. Jose, and C. E. Hamilton-Giachritsis, "Characteristics and behaviors of anonymous users of dark web platforms suspected of child sexual offenses," *Front. Psychol.*, vol. 12, p. 623668, 2021.

[26] J. Saleem, R. Islam, and M. Z. Islam, "Darknet traffic analysis: A systematic literature review," *IEEE Access*, vol. 12, pp. 42423–42452, 2024.

[27] U. Gasper, "Ethical and societal issues of automated dark web investigation: Part 5," *Dark Web Investig.*, pp. 189–233, 2021.

[28] O. C. Stringham *et al.*, "A guide to using the internet to monitor and quantify the wildlife trade," *Conserv. Biol.*, vol. 35, no. 4, pp. 1130–1139, 2021.

[29] C. Elendu *et al.*, "Ethical implications of AI and robotics in healthcare: A review," *Medicine (Baltimore).*, vol. 102, no. 50, p. e36671, 2023.

[30] K. Korre, A. Muti, and A. Barrón-Cedeño, "The challenges of creating a parallel multilingual hate speech corpus: An exploration," in *Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024)*, 2024, pp. 15842–15853.

[31] A. S. Rajawat *et al.*, "Dark web data classification using neural network," *Comput. Intell. Neurosci.*, vol. 2022, no. 1, p. 8393318, 2022.

[32] S. Samtani, W. Li, V. Benjamin, and H. Chen, "Informing cyber threat intelligence through dark web situational awareness: The AZSecure hacker assets portal," *Digit. Threat. Res. Pract.*, vol. 2, no. 4, pp. 1–10, 2021.

[33] Y. Niu, L. Ying, J. Yang, M. Bao, and C. B. Sivaparthipan, "Organizational business intelligence and decision making using big data analytics," *Inf. Process. Manag.*, vol. 58, no. 6, p. 102725, 2021.

[34] J. H. Awan, S. Memon, R. A. Khan, A. Q. Noonari, Z. Hussain, and M. Usman, "Security strategies to overcome cyber measures, factors and barriers," *Eng. Sci. Technol. Int. Res. J,* vol. 1, no. 1, pp. 51–58, 2017.

[35] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: A review," *Authorea Prepr.,* 2022.

[36] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya, and S. Khan, "Offensive security: Cyber threat intelligence enrichment with counterintelligence and counterattack," *IEEE Access,* vol. 10, pp. 108760–108774, 2022.

[37] R. Hazra, P. Chatterjee, Y. Singh, G. Podder, and T. Das, "Data encryption and secure communication protocols," in *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning*. IGI Global, 2024, pp. 546–570.

[38] M. Sain, O. Normurodov, C. Hong, and K. L. Hui, "A survey on the security in cyber physical system with multi-factor authentication," in *2021 23rd International Conference on Advanced Communication Technology (ICACT),* 2021, pp. 1–8.

[39] H. A. Al-Ofeishat, and R. Alshorman, "Build a secure network using segmentation and micro-segmentation techniques," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 1–16, 2023.

[40] S. Samtani, Y. Chai, and H. Chen, "Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model," *MIS Q.*, vol. 46, no. 2, 2022.

[41] D. Chatziamanetoglou, and K. Rantos, "Cyber threat intelligence on blockchain: A systematic literature review," *Computers*, vol. 13, no. 3, p. 60, 2024.

[42] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," *Comput. Secur.*, vol. 132, p. 103352, 2023.

[43] P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, and E. Foo, "Current approaches and future directions for cyber threat intelligence sharing: A survey," *J. Inf. Secur. Appl.*, vol. 83, p. 103786, 2024.

[44] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: An overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 173, 2021.

[45] I. Böhm, and S. Lolagar, "Open source intelligence: Introduction, legal, and ethical considerations," *Int. Cybersecurity Law Rev.*, vol. 2, no. 2, pp. 317–337, 2021.

[46] R. Rawat, B. Garg, V. Mahor, S. Telang, K. Pachlasiya, and M. Chouhan, "Organ trafficking on the dark web - The data security and privacy concern in healthcare systems," *Internet Healthc. Things Mach. Learn. Secur. Priv.*, pp. 189–216, 2022.