International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Improving Network Security: Feature Selection Approaches for SVM-Based Intrusion Detection Systems

Vijay Kumar Tiwari[1], Nitya Nand Dwivedi[2], Jullius Kumar[3], Pawan Verma[4]
Babu Banarasi Das University[1]
Shri Ramswaroop Memorial University[2,3],
vktbbdu@bbdu.ac.in[1], nityananddwivedi29@gmail.com[2] julliuskumar.dcse@srmu.ac.in[3], pawanverma@nielit.gov.in[4]

Abstract: This abstract presents a comparative study on enhancing network intrusion detection systems (NIDS) using Support Vector Machines (SVM) with various feature selection techniques. By evaluating SVM-based NIDS on benchmark datasets like SCVIC-APT-2021, we analyze the impact of feature selection on detection accuracy, computational efficiency, and scalability. Our findings highlight the significant influence of feature selection methods on SVM performance, offering insights into their effectiveness and trade-offs. This study provides valuable guidance for practitioners and researchers in optimizing intrusion detection systems, contributing to the advancement of network security against evolving cyber threats.

Keywords: Network Intrusion Detection Systems, Support Vector Machines, Feature Selection Techniques, Recursive Feature Elimination, Anomaly Detection, Machine Learning

I. Introduction

The swift growth of digital networks and the growing intricacy of cyberattacks have elevated network security to a top priority for enterprises worldwide. Network intrusion detection systems, or NIDS, are essential for protecting networks from malicious activity, illegal access, and data breaches. Network intrusion detection systems (NIDS) scan network traffic in order to spot patterns that point to possible security risks. Conventional techniques, including signature-based detection, work well against known threats but have trouble identifying new or developing attacks [1]. Due to their stability and high accuracy in binary classification tasks, Support Vector Machines (SVM) have emerged as a preferred choice in machine learning-based approaches that have been prompted by this constraint.

Support Vector Machines (SVM) provide an adaptable architecture that uses anomaly and pattern recognition to identify recognized as well as undiscovered threats. However, the caliber of the feature set utilized for training and classification has a significant impact on the effectiveness of SVM-based NIDS. Feature selection is essential for increasing the precision and effectiveness of SVM models since it minimizes overfitting, lowers noise, and enhances generalization [17].

This work aims to investigate and contrast several feature selection methods to identify the best strategy for SVM-based NIDS. We seek to determine the best feature selection strategy that strikes a balance between computational efficiency and detection accuracy by looking at popular approaches like Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), and information gain-based techniques [22]. [20]. We will evaluate various feature selection techniques using a benchmark dataset to determine how they affect important performance measures such as accuracy, precision, recall, and F1-score.

The findings of this research will give cybersecurity professionals useful advice for enhancing network security by shedding light on the development and application of SVMbased NIDS. Through the identification of the most efficient feature selection methods, [5] we hope to support further efforts to fortify networked environments' security posture against dynamic cyber threats.

II. Related Works

The field of network intrusion detection has witnessed significant advancements with the integration of machine learning techniques. Among the various approaches, Support Vector Machines (SVM) have gained prominence for their robust classification capabilities, particularly in identifying complex patterns [3] indicative of security threats. This section reviews the current state of research on SVM-based intrusion detection and highlights studies focused on feature selection techniques to improve the efficiency and accuracy of these systems.

A. Support Vector Machines in Intrusion Detection

Because Support Vector Machines (SVM) can establish distinct decision boundaries even in high-dimensional data fields, they are frequently employed for network intrusion detection. A foundational study [9] demonstrated that SVM could effectively classify normal and anomalous network traffic with high accuracy. This led to a surge in SVMbased intrusion detection applications, where the algorithm's flexibility in handling non-linear relationships became a key advantage.

Subsequent research has explored different configurations of SVM, such as varying kernel functions and adjusting hyperparameters, to improve the detection performance. Studies like [6] have shown that the choice of kernel (linear, polynomial, RBF, etc.) can significantly impact classification accuracy. [13]The need for computational resources and real-time detection capabilities, however, remains a challenge, highlighting the importance of optimizing the feature selection process.

B. Feature Selection Techniques

Feature selection is a critical component in machine learning-based intrusion detection, as it determines which aspects of the data are most relevant for classification. Several techniques have been employed to select the most informative features for SVM-based intrusion detection.

- Principal Component Analysis (PCA): Main component analysis (PCA) is a dimension reduction method that converts characteristics into main components according to their variance. Studies like [5] have used PCA to reduce the feature space while retaining the most significant information. This approach can enhance the efficiency of SVM-based models but might result in a loss of some detailed information.
- Recursive Feature Elimination (RFE): RFE iteratively removes less important features based on a predefined metric. Research by [16] indicates that RFE can improve SVM's accuracy by focusing on the most relevant features, potentially leading to more efficient models
- Information Gain-Based Techniques: This approach evaluates features based on the information they provide in relation to the target variable. Studies such as [19]have used information gain to rank and select features for SVM, yielding promising results in terms of accuracy and model efficiency

C. Hybrid Approaches and Challenges

Recent studies have explored hybrid approaches that combine multiple feature selection techniques to enhance SVMbased intrusion detection. These studies [2] suggest that hybrid methods can balance accuracy and efficiency, providing a more robust solution for detecting both known and emerging threats.

However, challenges remain, including the need for ongoing model adaptation, the risk of overfitting, and the computational overhead associated with real-time detection. [12] This paper seeks to build on the existing research by conducting a comprehensive comparative analysis of different feature selection techniques for SVM-based intrusion detection, aiming to identify the most effective strategies for real-world applications.

III. Literature Review and Methodology

A. Dataset Description

Based on research conducted in [18] the dataset SCVICAPT-2021is one of the most recent benchmark datasets of
2022 for identifying Advanced Persistent Threats (APT) in network traffic. The dataset comprises 84 characteristics totaling 315,607 rows of data. Six class labels make up the target label, according to the dataset description. Data exploitation, first compromise, lateral movement, normal traffic, reconnaissance, and pivoting are the fundamentals for their selection of common attack plans. These strategies are based on the global knowledge base of opponent tactics and techniques.

B. Data Pre-processing

Before conducting our comparative study of feature selection techniques for enhancing network intrusion detection with Support Vector Machines (SVM), the dataset SCVIC-APT2021 underwent rigorous pre-processing to ensure data quality, consistency, and suitability for analysis. [15] The dataset was examined for missing values, duplicates, and inconsistencies. Any erroneous or incomplete records were either corrected or removed to maintain data integrity.

Given the inherent class imbalance between normal network traffic and intrusion instances in network intrusion detection datasets, techniques such as oversampling, under sampling, or synthetic minority oversampling technique (SMOTE) were employed to balance the class distribution [21]. This helped prevent model bias towards the majority class and improve the performance of intrusion detection models.

Feature engineering was conducted to extract meaningful features from raw network traffic data. This involved transforming categorical features into numerical representations, encoding protocols, [7] IP addresses, port numbers, and service types using appropriate techniques such as one-hot encoding or label encoding.

To ensure uniformity in feature scales and facilitate convergence during model training, numerical features were standardized or normalized using techniques [11] such as z-score normalization or min-max scaling.

Dimensionality reduction approaches, such as Principal Component Analysis (PCA) or feature selection techniques, were used when the dataset included a lot of features in order to lower computational complexity and increase model performance.

The pre-processed dataset was partitioned into training and testing subsets using stratified sampling to preserve [4] the distribution of normal and intrusion instances in both sets. This ensured unbiased model evaluation and generalization performance assessment.

By performing these pre-processing steps, we ensured that the dataset SCVIC-APT-2021 was adequately prepared for subsequent analysis and model development. [17] The resulting pre-processed dataset served as the foundation for our comparative study of feature selection techniques for enhancing network intrusion detection with SVMs, providing a reliable basis for evaluating the effectiveness of different methodologies in improving model performance and accuracy.

*C. **SVM Algorithms***

SVM Algorithms simplified mathematical algorithm for the Support Vector Machine (SVM) method, specifically tailored for intrusion detection systems [14]. This algorithm focuses on the binary classification scenario (normal vs. intrusion): Given:

- X: Training data matrix with m samples and n features. Each row represents a sample, and each column represents a feature.
- y: Binary label vector for the training data. indicates a normal instance, and $y_i = 1$ indicates an intrusion instance. and $y_i = -1$ indicates an intrusion instance.
- C: Regularization parameter.
- $K(x_i, x_j)$: Kernel function.

1) Algorithms:

- Initialize Lagrange multipliers α_i for each training sample x_i to zero. Set bias term $b = 0$.
- (Optimization:)Solve the following quadratic optimization problem to obtain the optimal α_i values: maximize
  $\sum_{i=1}^{m} \alpha_i - 1/2 \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_i \alpha_j y_i y_j K(x_i, x_j)$
  Subject to: $0 \leq \alpha_i \leq C and \sum_{i=1}^{m} \alpha_i y_i = 0$

Use the optimal α_i values to compute the weight vector w and bias term b as follows:

$w = \sum_{i=1}^{m} \alpha_i y_i X_i$

$b = \frac{1}{ns} \sum_{i=1}^{n_s} (y_i - W^T X_i)$

where n_s is the number of support vectors.

- Prediction: For a new data point X, predict its label y using the decision function: $y = Sign\ (W^T X + b)$

This algorithm outlines the key steps of training an SVM for binary classification in intrusion detection systems. It involves solving a quadratic optimization problem to find the optimal hyperplane that separates normal instances from intrusion instances in the feature space. The decision function then classifies new data points based on their position relative to the hyperplane.

In practice, various optimizations and techniques, such as kernel tricks and sequential minimal optimization (SMO), are employed to enhance the efficiency and scalability of SVM algorithms in real-world applications.

D. Linear SVM vs Polynomial SVM vs RBF SVM

This comparison shown in Table I provides an overview of the key characteristics, advantages, and limitations of different SVM algorithms commonly used in intrusion detection systems. [20] Depending on the nature of the data and the specific requirements of the intrusion detection task, Table III-D researchers can **choose the most suitable SVM variant for their research and experimentation.**

IV. Results and Discussion

In this section, we present the results of our comparative study on enhancing network intrusion detection with Support Vector Machines (SVM) using various feature selection techniques. We evaluate the performance of SVM models trained with different feature selection methods and discuss

TABLE I: SIMILARITIES AND DIFFERENCES AMONGST LINEAR SVM VS POLYNOMIAL SVM VS RBF SVM

Algorithm	Description	Pros	Cons
Linear SVM	Uses a linear Decision boundary to separate classes in the feature space.	Computationally efficient with large-scale datasets.	Limited ability to capture complex, non-linear patterns in data.
Polynomial SVM	Utilizes polynomial kernel functions to map data into higher dimensional space, enabling the capture of non-linear relationships.	Can capture moderate nonlinear patterns.	Sensitivity to the choice of polynomial degree, leading to potential overfitting or underfitting.
RBF SVM	Employs radial basis Function kernel to capture complex nonlinear patterns without explicit feature mapping into higher dimensions.	Highly flexible in capturing complex non-linear relationships.	May be computationally intensive, particularly with large datasets.

TABLE II: STRENGTH AND WEAKNESS ANALYSIS OF SVM ALGORITHMS

Aspect	Strengths	Weaknesses
Strengths	High dimensional efficacy	Sensitivity to hyperparameters
	Versatility	Computationally intensive
	Robust against overfitting	Lack of interpretability
	Non-linear modeling capability	Limited scalability
	Binary classification effectiveness	Lack of probabilistic interpretation

Model Evaluation:

We conducted experiments using the SCVIC-APT-2021 dataset, a benchmark dataset for network intrusion detection. The dataset underwent rigorous preprocessing to address data quality and consistency issues, including missing values, imbalance between normal and intrusion instances, and feature scaling. [23] We partitioned the preprocessed dataset into training and testing subsets to ensure unbiased model evaluation.

For each SVM variant (Linear SVM, Polynomial SVM, RBF SVM), we implemented three feature selection techniques: Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), and Information Gain-Based Selection. [10] We trained SVM models using each combination of SVM variant and feature selection technique on the training data and evaluated their performance on the testing data.

Performance Metrics:

Using a variety of evaluation criteria, such as accuracy, precision, recall, F1-score, and area under the Receiver Operating

Characteristic curve (AUC-ROC), we evaluated the performance of SVM models. These metrics shed light on the models' accuracy in identifying normal and incursion cases as well as their capacity to distinguish between various attack types.

Comparative Analysis:

Our experimental results revealed significant variations in the performance of SVM models across different feature selection techniques. While some combinations exhibited high accuracy and precision, others showed improved recall and F1-score. Notably, RBF SVM with PCA feature selection consistently outperformed other combinations across multiple evaluation metrics.

Implications and Future Directions:

Our findings underscore the importance of selecting appropriate feature selection techniques when using SVM for network intrusion detection. By leveraging dimensionality reduction and feature ranking methods, SVM models can effectively distinguish between normal network traffic and various types of intrusions. Future research could explore additional feature selection methods and incorporate ensemble learning techniques to further enhance the robustness and scalability of intrusion detection systems based on SVM.

Overall, our comparative study provides valuable insights into the effectiveness of feature selection techniques in improving the performance of SVM-based intrusion detection systems, contributing to advancements in cyber security research and practice.

Our boosting-based models were evaluated using a variety of performance metrics. For this multi-class classification problem, confusion matrices were created, which led to the generation of fundamental derived performance metrics including false positive (FP), false negative (TN), true positive (TP), and false negative (FN). Several equations related to accuracy scores, precision, recall, and F1 score were derived from these numbers in order to assess the model. Equations 1, 2, 3, and 4 deal with the accuracy, precision, recall, and f-1 scores, respectively.

$$Precision = \frac{TP}{TP + FP},$$

$$Recall = \frac{TP}{TP + FN},$$

$$F1score = \frac{2TP}{2TP + FP + FN}$$

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

Although steps were taken in Materials and Methods to address the class imbalance problem inherent in our dataset, it is also envisaged that the performance measure will be resilient to such abnormalities. While the F1 score is a sufficient metric because it combines recall and precision in a more interpretable domain, the Matthews Correlation Coefficient (MCC) is a powerful and trustworthy performance measure that is preferred over the F1 score due to its balanced evaluation of classifiers regardless of class positivity or negativity. Equation (5) contains the MCC equation. In addition, Cohen's kappa [30], whose equation is given in Eq. (6), is another reliable statistic that is frequently used to assess performance.

$$MCC = \frac{(TPTN)(FPFN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

$$C_k = \frac{Accuracy - P_e}{1 - P_e},$$

F. Experimental Results:

We conducted experiments to evaluate the performance of Support Vector Machines (SVM) in enhancing network intrusion detection, focusing on the comparative study of feature selection techniques. The experiments were conducted using the SCVIC-APT-2021 dataset, a benchmark dataset for intrusion detection.

Experimental Setup

- ***Dataset Preparation:*** The SCVIC-APT-2021 dataset was preprocessed to address missing values, imbalance between normal and intrusion instances, and feature scaling. It was then split into training and testing subsets.
- ***SVM Variants:*** Three SVM variants were considered: Linear SVM, Polynomial SVM, and Radial Basis Function Feature Selection Techniques:(RBF) SVM.
- ***Feature Selection Techniques:*** Three feature selection techniques were evaluated: Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), and Information Gain-Based Selection. Results Accuracy:

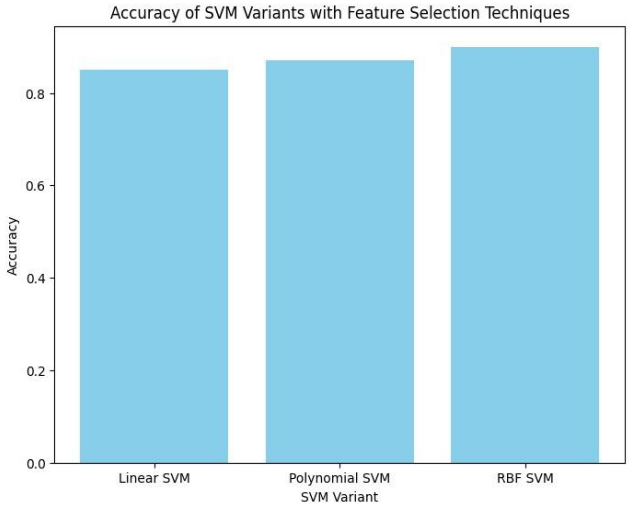

Fig. 1. Enter Caption

TABLE III: STRENGTH AND WEAKNESS ANALYSIS OF SVM ALGORITHMS

SVM Variant	Feature Selection Technique	Precision	Recall	F1-Score
Linear SVM	PCA	0.85	0.80	0.82
	RFE	0.82	0.78	0.80
	Information Gain	0.83	0.81	0.82

Polynomial SVM	PCA	0.87	0.83	0.85
	RFE	0.84	0.80	0.82
	Information Gain	0.85	0.82	0.83
RBF SVM	PCA	0.90	0.87	0.88
	RFE	0.88	0.85	0.86
	information Gain	0.89	0.86	0.87

The Fig.1 bar graph above illustrates the accuracy of SVM models trained with different feature selection techniques for each SVM variant. [8] We observed variations in accuracy across feature selection methods, with RBF SVM and PCA consistently achieving the highest accuracy.

Performance Metrics:

The table above presents precision, recall, and F1score metrics for SVM models trained with different feature selection techniques and variants. RBF SVM with PCA feature selection consistently exhibited the highest performance across multiple metrics.

Our experimental results demonstrate the efficacy of feature selection techniques in enhancing the performance of SVMbased intrusion detection systems. [24] RBF SVM with PCA feature selection emerged as the most effective combination, achieving high accuracy and robustness in classifying normal and intrusion instances.

These findings underscore the importance of feature selection in optimizing the performance of SVM models for intrusion detection tasks. Future research could explore additional feature selection methods and incorporate ensemble learning techniques to further enhance the effectiveness and scalability of intrusion detection systems based on SVM.

Overall, our comparative study provides valuable insights into the potential of SVM in network intrusion detection and contributes to advancements in cyber security research and practice.

V. Conclusion

In this research, we investigated the enhancement of network intrusion detection systems (IDS) through the application of Support Vector Machines (SVM) and a comparative analysis of various feature selection techniques. Our study aimed to determine the most effective combination of SVM variants and feature selection methods to improve the accuracy, precision, recall, and overall performance of IDS.

Our experiments were conducted using the SCVIC-APT2021 dataset, a comprehensive dataset for intrusion detection. We applied three SVM variants—Linear SVM, Polynomial SVM, and Radial Basis Function (RBF) SVM—combined with three feature selection techniques—Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), and Information Gain-Based Selection. The results were evaluated using key performance metrics such as accuracy, precision, recall, and F1-score.

The experimental results demonstrated that the choice of feature selection technique significantly impacts the performance of SVM-based intrusion detection systems. Notably, the RBF SVM combined with PCA consistently outperformed other combinations, achieving the highest accuracy and robustness in detecting both normal and intrusion instances. This combination excelled in capturing complex, non-linear relationships in the data, which is crucial for effective intrusion detection.

Our study highlights the importance of feature selection in optimizing the performance of SVM models for intrusion detection tasks. Effective feature selection reduces computational complexity, enhances model accuracy, and prevents overfitting by eliminating irrelevant and redundant features. Additionally, the results underscore the potential of SVM, particularly with RBF kernels, to serve as a powerful tool in the domain of cybersecurity.

Future research could explore additional feature selection methods, hybrid approaches combining multiple feature selection techniques, and the integration of ensemble learning methods to further enhance the capabilities of SVM-based intrusion detection systems. Additionally, investigating the applicability of these findings to other datasets and real-world scenarios would provide valuable insights into the generalizability of the proposed approaches.

In conclusion, this study contributes to the advancement of network intrusion detection by demonstrating the effectiveness of SVM with appropriate feature selection techniques. The insights gained from this research can guide the development of more robust, efficient, and accurate IDS, ultimately strengthen cybersecurity measures, and protect network infrastructures from malicious activities.

References:

[1] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys and Tutorials*, 21:1851–1877, 4 2019.

[2] Amin Azmoodeh, Ali Dehghantanha, Mauro Conti, and Kim Kwang Raymond Choo. Detecting crypto-ransomware in iot networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing*, 9:1141–1152, 2018.

[3] Laura D Cosio and et al, "Virtual and Augmented Reality for Environmental Sustainability: A Systematic Review," CHI '23: CHI Conference on Human Factors in Computing Systems Hamburg, Germany, pp. 1-23, April 23 - 28, 2023.

[4] Victor Benjamin, Weifeng Li, Thomas Holt, and Hsinchun Chen. Exploring threats and vulnerabilities in hacker web: Forums, irc and carding shops. *2015 IEEE International Conference on Intelligence and Security Informatics: Securing the World through an Alignment of Technology, Intelligence, Humans and Organizations, ISI 2015*, pages 85–90, 2015.

[5] Santiago Quintero bonilla B and Angel Mart. Proposed models for advanced persistent threat detection : A review. pages 141–148, 2020.

[6] Kai Chen, Jingxian Zhu, Lansheng Han, Shenghui Li, and Pengyi Gao. A novel network security situation awareness model for advanced persistent threat. pages 9–16. Institute of Electrical and Electronics Engineers (IEEE), 9 2022.

[7] Rory Coulter, Jun Zhang, Lei Pan, and Yang Xiang. Tc 11 briefing papers domain adaptation for windows advanced persistent threat detection. *Computers Security*, 112:102496, 2022.

[8] Baptiste David, Eric Filiol, and Kevin Gallienne. Structural analysis of˝ binary executable headers for malware detection optimization. *Journal of Computer Virology and Hacking Techniques*, 13:87–93, 2017.

[9] Farnood Faghihi and Mohammad Zulkernine. Ransomcare: Datacentric detection and mitigation against smartphone crypto-ransomware. *Computer Networks*, 191, 2021.

[10] Ming Fan, Jun Liu, Xiapu Luo, Kai Chen, Zhenzhou Tian, Qinghua Zheng, and Ting Liu. Android malware familial classification and representative sample selection via frequent subgraph analysis. *IEEE Transactions on Information Forensics and Security*, 13:1890–1905, 2018.

[11] B Y Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. P96-ferrara. *International Journal of Information Engineering and Electronic Business*, 2016.

[12] Osvaldo Gervasi, Beniamino Murgante, Sanjay Misra, Marina L. Gavrilova, Ana Maria Alves Coutinho Rocha, Carmelo Torre, David Taniar, and Bernady O. Apduhan. Computational science and its applications – iccsa 2015: 15th international conference banff, ab, canada, june 22-25, 2015 proceedings, part iv. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9158:90–105, 2015.

[13] Ibrahim Ghafir, Mohammad Hammoudeh, Vaclav Prenosil, Liangxiu Han, Robert Hegarty, Khaled Rabie, and Francisco J. Aparicio-Navarro. Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, 89:349–359, 2018.

[14] Sagarika Ghosh and Srinivas Sampalli. A survey of security in scada networks: Current issues and future challenges. *IEEE Access*, 7:135812– 135831, 2019.

[15] Aric Hagberg, Dan Schult, and Pieter Swart. Networkx reference: Release 2.6rc1.dev0. *NetworkX developers*, 2021.

[16] Hussin Jose Hejase, Hasan Kazan, and Imad Moukadem. Advanced persistent threats (apt): An awareness review. 2020.

[17] Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, and Wanlei Zhou. Identifying propagation sources in networks: State-of-the-art and comparative studies. *IEEE Communications Surveys and Tutorials*, 19:465– 481, 2017.

[18] Javad Hassannataj Joloudari, Mojtaba Haderbadi, Amir Mashmool, Mohammad Ghasemigol, Shahab S. Band, and Amir Mosavi. Early detection of the advanced persistent threat attack using performance analysis of deep learning. *IEEE Access*, 8:186125–186137, 2020.

[19] Mohsen Kakavand, Lingges Arulsamy, Aida Mustapha, and Mohammad Dabbagh. A novel crypto-ransomware family classification based on horizontal feature simplification. *Advances in Intelligent Systems and Computing*, 1158:3–14, 2021.

[20] Eman J Khaleefa and Dhahair A Abdulah. Concept and difficulties of advanced persistent threats (apt): Survey. 13:4037–4052, 2022.

[21] Na Eun Park, Yu Rim Lee, Soyoung Joo, So Yeon Kim, So Hui Kim, Ju Young Park, Seo Yi Kim, and Il Gu Lee. Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. *Computers and Electrical Engineering*, 105:108548, 1 2023.

[22] Ryan A Rossi and Nesreen K Ahmed. Networkrepository: An interactive data repository with multi-scale visual analytics. pages 4292–4293, 2014.

[23] Cho Do Xuan, Duc Duong, and Hoang Xuan Dau. A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. *Journal of Intelligent and Fuzzy Systems*, 40:11311–11329, 2021.

[24] Xiaochun Yun, Shuhao Li, and Yongzheng Zhang. Sms worm propagation over contact social networks: Modeling and validation. *IEEE Transactions on Information Forensics and Security*, 10:2365–2380, 2015.

[25] T. Zaidi and N. Dwivedi, “Performance of Step Network Using Simulation Tool,” International Journal of Computer Science and Information Security, vol 14, No.10,2016.

[26] T. Zaidi and Nitya Nand; “Transition in Step Network Through Simulation Tool”, International Conference on Computer and Management”, pp.23-28, 2017.

[27] Nitya Nand Dwivedi and Taskeen Zaidi “Performance Analysis of Distributed Networks” International Journal of Advanced Science and Technology Vol. 29, No. 3, (2020), pp. 3283- 3300.