International Journal of Core Engineering & Management

Volume-7, Issue-04, 2022 ISSN No: 2348-9510

ADVANCEMENTS IN CYBERSECURITY: EVALUATING MACHINE LEARNING APPROACHES FOR DETECTING CYBER ATTACKS

Dhaval Gogri
dhaval.gogri17@gmail.com

Abstract

With the popularization and application of Internet technology, people can easily steal valuable information from cyber attackers using computer networks and electronic products. With the rise of sophisticated cyberattacks, the efficiency of intrusion detection systems becomes paramount. In the modern world, IDS integrated systems that support machine study can predict and detect potential violations of security. As discussed in this paper, there is a proposed machine learning approach to the detection of computer network intrusion. The five main steps of the proposed method are feature selection, splitting, normalization, preprocessing, and classification. The Random Forest Based Feature Selection technique selects the most crucial characteristics. The K-Nearest Neighbor (KNN) enhances Cybersecurity for Detecting Cyber Attacks. The application of the proposed method was done on the large-scale data set, that is, the NSL-KDD network attack data set. The study evaluates one model and several sub-models including K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) for its intrusion detection features. When using f1-score, recall, accuracy, precision, ROC, as well as confusion matrix to measure the performance of the chosen machine learning model. Regarding accurately classifying traffic and identifying intrusions, the KNN model outperformed the others with a 98.24% accuracy, 97.99% accuracy, 98.00% F1-score, and 97.91% recall. According to the experimental data, the recommended approach works better than the other machine learning algorithms and has a high detection rate for properly classifying intrusions.

Keywords: Cybersecurity, cyber-attacks, network attacks, NSL-KDD, Machine Learning, K-Nearest Neighbors (KNN).

I. INTRODUCTION

Today, tools and techniques of hacking are on the rise due to the advancement in technology. Therefore, such increased vulnerabilities mean that many companies today require extra apparatus to guard against cybercrimes and fraudsters. However, one of the basic and yet challenging processes which are needed to predict and recognize an attack prior to its occurrence in cybersecurity is threat anticipation [1]. Different goals, sizes, and levels of complexity can result in various patterns and intensities of cybersecurity assaults. Because of this enormous diversity, organizations and nations must consider cyber security one of their core systems[2].

This shift compels organizations to consider modern and advanced methods to stay up to date with the evolution of cyberattacks. Thus, academics and security professionals are becoming more interested in a new generation of cybersecurity technologies that are in high demand[3]. Organizations can detect, prevent, and recover from cyberattacks by using the knowledge they have gathered to inform their cybersecurity decisions[4].

Artificial Intelligence and machine learning have become essential tools in the field of cybersecurity [5]. Using algorithms in cybersecurity frameworks signifies a paradigm change in defensive measures, moving away from traditional rule-based procedures and towards more proactive and adaptive approaches [6][7]. The awareness that traditional cybersecurity defenses, which mostly depend on static rule sets and signature-based detection systems, are losing ground against modern cyber threats' complex and dynamic nature is what spurred this development.[8]. Because AI and machine learning techniques offer the agility, scalability, and predictive skills required to effectively counter cyber-attacks, their integration holds great promise for strengthening cyber defenses[9]. The ability to use data power is fundamental to AI-driven cybersecurity[10][11].

Large-scale labelled and unlabelled data sets feed machine learning algorithms, enabling them to identify complicated patterns and anomalies that point to malicious activity in various challenging datasets [12][13]. These algorithms can detect subtle signs of compromise by examining past attack data, user activity, network traffic, and system logs. This allows for the early identification and mitigation of cyber-attacks before they cause significant harm. Furthermore, the adaptable nature of machine learning algorithms enables cybersecurity systems to change quickly in step with the evolving threat landscape [14]. Using ongoing learning and optimization, these algorithms improve their ability to identify new and undiscovered dangers, strengthening defenses against cyberattacks. This flexibility is especially important when dealing with highly skilled cyber adversaries that use polymorphic, covert, and zero-day attack methods to avoid detection[15][16]. To improve cybersecurity, In this research, the NSL-KDD dataset—a well-liked dataset for training and testing intrusion detection models—is used to demonstrate the use of models for machine learning.

1. Contributions of the Study:

This study substantially advances the intrusion detection domain by thoroughly analyzing machine learning techniques using the NSL-KDD dataset to detect and evaluate network breaches. The key contributions are as follows:

- It contributes to understanding the strengths and weaknesses of both ML and DL approaches in intrusion detection, guiding upcoming studies and advancements in cyberattack detection.
- By utilizing the NSL-KDD dataset, the study offers an in-depth analysis of network-based attacks, reflecting real-world intrusion detection challenges.
- This study provides the basis for model evaluation criteria and a benchmark for the next research to grasp IDS, which include accuracy, precision, recall, and F1-score.
- This research improves intrusion detection systems where the concept of the feature of this selection and data pre-treatment is clearly demonstrated to have a profound effect on the model's precision and stability.

2. Organization of the paper

The research is then organized. The current literature on intrusion detection is presented in Sections I and II, emphasizing the gaps and advancements in the field. Section III outlines the study's methodology. Section V offers the conclusion and future implications, while Section IV outlines the findings and discussion. The conclusion and possible course of action are outlined in the closing section.

II. LITERATURE REVIEW

The previous research on effective intrusion detection through the application of deep learning and machine learning techniques is presented in this part.

Wang et al. (2019) An attack classifier based on ensemble learning technique using extreme gradient boosting method. The effectiveness of the proposed classifier is assessed through an experiment on a physical cyber system dataset collected from a HWIL smart grid testbed. The classification accuracy rises beyond 99% – demonstrating an improvement of the proposed solution by 4% compared to the cutting-edge while preserving the higher-than-95% level of accuracy in more complicated and qualitatively changing conditions [17].

Dehghani et al. (2021) The proposed detection approach involves wavelet singular entropy analysis of temporally successive system states. Breaking down the switching surface by a sliding-mode controller requires altering singular value matrices and certain wavelet transform coefficients; predicted entropy values are then computed via a process that is stochastic. Identifying assaults is accomplished by the WSE by the establishment of indices that are based on the levels of voltage and current switching. The simulation results confirm the higher efficacy of the suggested FDIA finding approach. This exposure system can attain an accuracy rate above 96.5% and is distinguished by its quick detection capabilities (10 milliseconds post-assault beginning) [18].

Verma et al. (2021) train a binary classifier utilizing a GBM ensemble technique for anomaly detection and preventing zero-day attacks on Internet of Things networks. The obtained metrics for the positive class were as follows: recall 95.70%., precision 96.40%, and accuracy 98.27%. The simulation outcomes demonstrate how well the suggested method mitigates cyberattacks, making it appropriate for critical Internet of Things applications[19].

Alsulami and Zein-Sabatto (2021) Innovative and robust security methodology for identifying and countering sensor spoofing cyber-attacks on ACPS. A cyber-attack detection system was created to locate and eliminate questionable communication packets from aviation network traffic using the Artificial Immune System's (AIS) positive selection process. After a final integration, the NCS and detection system were evaluated in actual cyber-security assault scenarios. Using the True Positives and True Negatives rates, the algorithm achieved an accuracy of 0.96. Based on linear regression analysis, the coefficient of determination (R-value) showed that the NARX's estimated accuracy was 0.99 [20].

Al-Abassi et al. (2020) The deep learning model could be used to build equal, distinct representations of imbalanced datasets. The proposed attack detection approach employs the purpose of detecting cyber assaults from a variety of representations, DNN and DT. The results confirm that the suggested method is superior to newer models described in the literature and traditional classifiers such as Random Forest (RF), Deep Neural Networks (DNN), and AdaBoost [21]. The subsequent Table 1 summarizes the pertinent research on detecting cyber-attacks with machine learning methodologies.

Table 1: Summary of the related work on the detection of cyber-attacks using machine-learning techniques

References	Methodology	Dataset	Performance	Limitations & Future Work
Wang et al. [17]	A classifier for cyber-physical systems using an ensemble learning framework, specifically XGBoost.	Data was collected from a smart grid testbed employing a hardware-in-the-loop module to evaluate high-fidelity grid architectures.	Attained more than 99% classification accuracy, demonstrating a 4% improvement above the state-of-the-art, and maintained more than 95% accuracy in complex, dynamic situations.	Further, examination is needed to assess performance in diverse real-world conditions and with evolving attack vectors.
Dehghani et.al. [18]	WSE, a play on wavelet singular value decomposition (SVD), is used to detect FDI threats from cyberspace.	Applied to various case studies with different types of false data injection.	Capable of fast detection (10 ms from attack initiation) with an accuracy rate of over 96.5%.	Future work could explore the method's effectiveness in larger, more complex systems and its integration with other detection techniques.
Verma et.al. [19]	Gradient Boosting Machine (GBM) ensemble methodology for IoT network security.	Utilized pre-processed data packets.	The model achieved 98.27% accuracy, 96.40% precision, and 95.70% recall in detecting anomalies.	Further research could focus on adapting the model to various IoT environments and evaluating its performance against emerging threats.
Alsulami and Zein-Sabatto[20]	Artificial Immune System (AIS) based detection and defense protocol against sensor spoofing in aviation cyber-physical systems.	Evaluated in authentic cyber-security attack scenarios within an aviation Networked Control System (NCS) simulation.	The algorithm attained an accuracy of 0.96, determined by True Positive and True Negative detection rates.	Future work may involve enhancing the system's adaptability to various attack types and integrating it with other security measures.
Al-Abassi et.al. [21]	Ensemble deep learning model combining DNN and Decision Trees (DT) for attack detection in ICS.	Assessed on two authentic ICS datasets with 10-fold cross-validation.	The proposed technique surpassed traditional classifiers like RF, DNN, and AdaBoost.	Further studies could investigate the model's scalability and effectiveness in real-time applications.

III. METHODOLOGY

In this methodology, effective detection and prevention mechanisms must be implemented due to cyberattacks' increasing frequency and sophistication. Since cyber dangers can seriously hurt both persons and enterprises, they must be discovered properly and quickly. AI and ML, then, this research aimed at enhancing cyberattack detection through safety solutions to minimize these vices.

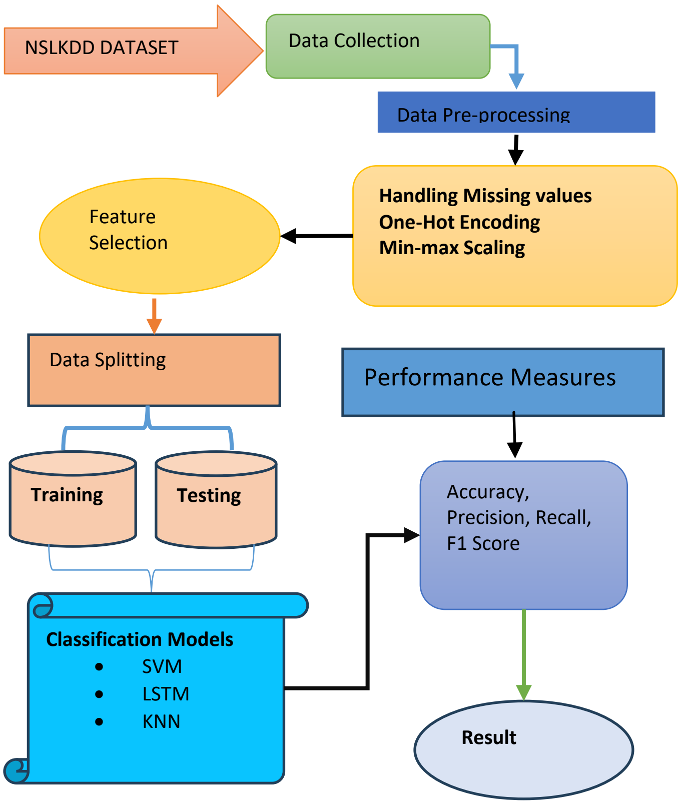

Figure 1: Proposed flowchart for the cyber security system

The methodology for detecting cyber-attacks for effective advancements in cybersecurity has several key steps, shown in Figure 1. The NSL-KDD dataset is employed in a stepwise intrusion detection algorithm. First, data collection is done, then pre-processing is done that consists of handling missing values, encoding technique using One-Hot and normalizing of data using Min-Max scaling. Then follows the feature selection process, which is used to retain only important characteristics of the intrusion detection process. Therefore, several classification models such as SVM or support vector machine LSTM and KNN have been deployed and assessed using the segmented data. In order to estimate which of these models is more applicable for intrusion detection, these models are evaluated by such parameters as accuracy coefficient, precision, recall, F1 measure, etc. The results produced are then analyzed. The following are the subsequent steps of the flowchart for the cyber security system proposed. The flowchart below outlines the flow of activities in the cyber security system:

1. Data Collection

This study looked at IDS using the NSL_KDD dataset made by the Canadian Institute for Cybersecurity at the University of New Brunswick. To mitigate model bias, the dataset, an enhanced iteration of KDD Cup 1999, removes redundant and duplicate entries. It identifies four primary types of intrusions: DoS, R2L, U2R, and probing, alongside standard traffic. The NSL-KDD-Train dataset is partitioned into two segments to mitigate overfitting: 25% (or 22,544 records) are set aside for validation, while 75% (or 125,973 records) are devoted to training. The validated models are evaluated against the NSL-KDD-Test+ dataset, which has 41 characteristics classified as 'normal' or 'intrusion.'

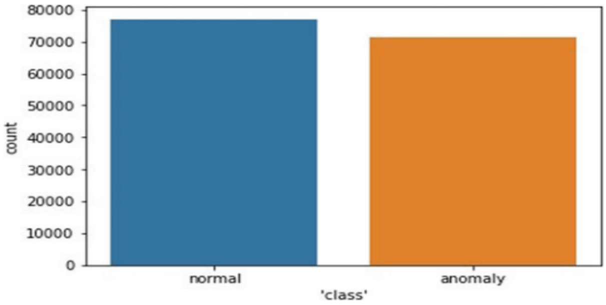

Figure 2: Quantities of standard and unconventional examples within a dataset.

Attacks fall into four different groups in the NSL_KDD collection. All of them are categorized as anomalies; normal falls into a different category. Figure 2 illustrates the numeral of occurrences within the normal and anomalous categories. The figure indicates stability among typical and anomalous instances. This indicates that the dataset employed is unbiased.

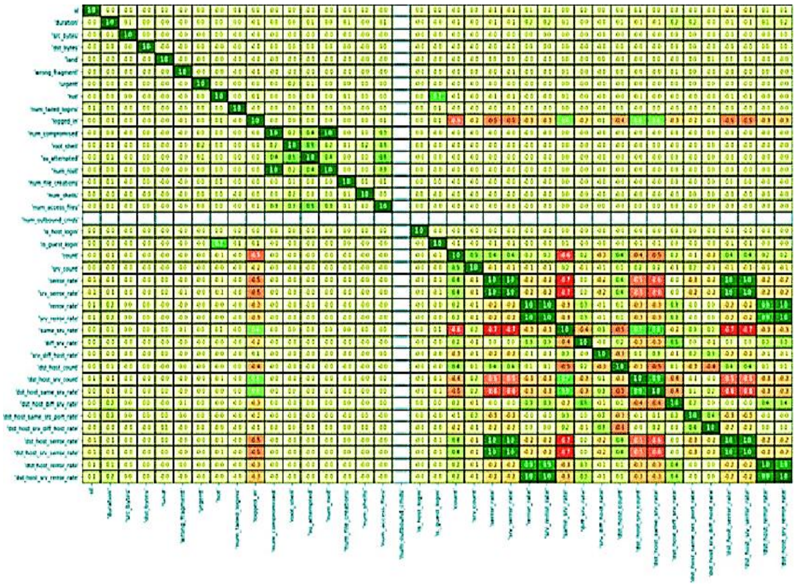

Figure 3: Heat map of the NSL-KDD dataset

A complete image of the event is also provided by the heat map, which allows for the visual display of value distribution pattern analysis. Figure 3 displays the NSL_KDD dataset's association heat map. This scatterplot illustrates the interdependence of the feature variables in the NSL_KDD dataset. In Figure 3, they are identified through labels such as ‘num_outbound_cmd,’ which gives an empty white box schematic with no data. The removal of this feature otherwise does not impede others that they still function properly. The diagonal value in the matrix that is not 1 is "num_outbound_cmds." Similarly, there is a connection between the corresponding columns. Consequently, the graph demonstrates that each feature is helpful for creating models.

2. Data Preprocessing

Data processing is a prerequisite for data analysis and for the proper operation of an intrusion detection system. There are four main components to the preparatory stage: cleaning the dataset by removing missing, null, or NaN values, feature selection, one-hot encoding, and normalization, ensuring consistency across the dataset and enhancing the effectiveness of models for machine learning.

A. Handling Missing values

The raw datasets had missing, null, or non-numeric (NaN) values that needed fixing. Initially, these distortions were detected, and the dataset's missing or null values were removed to guarantee data quality. Since clean data improves machine learning models' performance and accuracy, Preparing the dataset for additional processing and modelling was crucial.

B. One-Hot Encoding for labeling

This categorical data encoding technique applies when the characteristics are nominal and lack inherent order. In every level of a categorical characteristic in one-hot encoding, a new variable is generated, and each category is represented by a binary variable that has either 0 or 1. In this case, 0 denotes the absence of the category, while 1 denotes its presence.

C. Normalization using Min-max scaling

Normalization is a method to guarantee that every data within the database possesses a comparable range. This ithnue.;

$$X_{std} = \frac{(X-X.min)}{(X.min-X.min)} \tag{1}$$

$$X_{scaled} = X_{std} * (X.max - X.min) + X.\min \ldots \tag{2}$$

Here;

- X: The initial value or characteristic that needs to be normalized.
- Xmin: The dataset's lowest value for the functions X.
- X max: The highest value of the dataset's characteristic X.
- X std: The standardized value of X after applying Min-Max normalization.
- X scaled: The final scaled value that falls within the range of [0, 1].

3. Feature selection with random forest:

Feature selection improves machine learning precision, an important step in intrusion detection. Models by eliminating unnecessary data and identifying the most pertinent features. The Random Forest model was chosen because of its superior performance in feature selection and classification tasks. The Indeterminate Forest model ranks features according to their value, allowing you to pick the most important ones for better model performance.

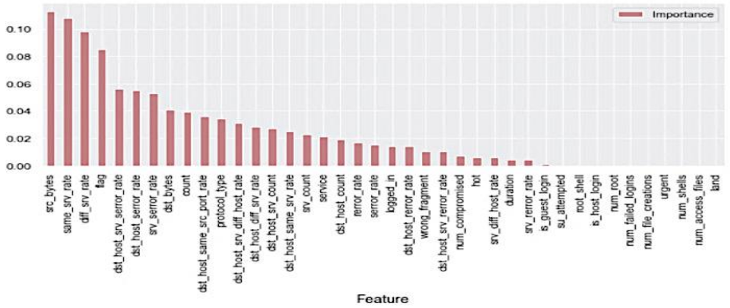

Figure 4: Significance of Features in the NSL_KDD

Dataset Subsequently, the optimal are chosen according to specific performance criteria. The significance of our features was assessed using RF, as depicted in Figure 4. RF is a procedure in which the algorithm operates recursively until the predetermined number of features is chosen. In the NSL-KDD procedure, RFE is utilized to acquire the requisite dataset. We identified the top 10 features utilizing the "n_features_to_select" parameter. In NSL-KDD, we removed redundant data by choosing a subset of pertinent features.

4. Data Splitting

Data partitioning is a crucial phase in data preprocessing. Initially the datasets were divided into subgroups for testing (30%) and training (70%).

5. Classification Models

This section discusses the Analysis and Classification of Intrusion Detection Models Utilizing Machine Learning Techniques:

A. Support Vector Machine (SVM)

An SVM is a unique classifier mathematically represented in a higher-dimensional space. Support Vector Machines (SVM) employ separate lines or graphs to categorize or differentiate between several classes or cases. Support Vector Machine (SVM) performs class division. Similar to kernel regression analysis, it employs lines to represent classifications. Vector Machines (SVMs) are a category of kernel-based categorization methodologies. Moreover, the SVM utilizes an objective that explicitly enhances classification efficacy [22].

B. Long Short-Term Memory (LSTM)

Recursive functions that call themselves repeatedly are comparable to recurrent functions. Neural networks are considered cyclical processes, including doing the same calculations on every dataset element. Recurrent Neural Networks (RNNs) are vulnerable to disappearing and ballooning gradient issues. Two RNN variations that lessen the challenges of traditional RNNs are LSTM and GRU. An LSTM is composed of an input gate, an output gate, and a forget gate consequently. The mathematical representations of the functionalities of the gates within an LSTM cell are presented as follows:

C. K-Nearest Neighbors (KNN)

An algorithm called K-Nearest Neighbors, or kNN, is a pattern recognition method that classifies objects by consulting the closest training instances within the attribute space. This algorithm classifies according to the designated k value about the class of the nearest neighbor. The kNN algorithm determines a vector's classification by utilizing known class vectors. Each sample in the training set is processed individually for testing. To ascertain the class of the sample under examination, the k nearest samples from the training set are identified. In the class of t-selected samples, the team analyzed is the class with the highest number of samples. This study employs the Euclidean criteria resented Eq. (3).

$$D_{L2}(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (3)$$

In this study, the distance significance for Nearest Neighbor is uniform, and the number of Neighbors is set at 10[23].

6. Model Evaluation

This article proposes a critique of four measures that are typically used in the analysis of the efficiency of the interruption-finding system. Ensuring the aforementioned parameters, five assessment metrics comprise precision, accuracy, Sensitivity, and F1-score, and four signs from the confusion matrix are TP, TN, FP and FN, all defined below. The confusion matrix has been presented in tabular form in Table 2 under.

Table 2: Confusion matrix

Predicted Attack	**Predicted**	**Normal**
Actual Attack	TP	FN
Actual Normal	FP	TN

- True Positive (TP): This relates to the count of singled-out examples classified into actual and expected positives.
- True Negative (TN): This has to do with the numeral of positive observations classified as negative.
- False Positive (FP): This relates to the numeral of negative observations but is expected to be positive.
- False Negative (FN): This means the numeral of positive reports that were anticipated to be negative.

A. Accuracy

Accuracy is a statistic for assessing categorization models, denoting the ratio of accurate predictions generated by the model, as illustrated in Equation 4:

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \quad (4)$$

B. Precision

Exactness is defined as follows in Equation 5: Precision = No of accurately identified positive outcome. Total no of positive results, including those incorrectly identified:

$$Precision = \frac{TruePositive}{(TruePositive+FalsePositive)} \quad (5)$$

C. Recall

The recall refers to the percentage ratio of accurately recalled outcome to the total sample that ought to be correctly recalled. It is also shown in the formula 6:

$$Recall = \frac{TruePositive}{(TruePositive+FalseNegative)} \quad (6)$$

D. F1-Score

The meaning of F1-Score, relating to the evenness between Precision and Recall, is to be used as criteria to model selection on this balance, as Equation 7:

$$F1\ score = \frac{2\times(Precision\times Recall)}{Precision+Recall} \quad (7)$$

These metrics assess how well machine learning models performed in identifying NSL-KDD cyberattacks and improving overall cybersecurity.

IV. RESULT ANALYSIS AND DISCUSSION

This section defines and deliberates the outcomes as well as the discussion on the presentation of the ML models that were applied to the NSL-KDD cyberattacks. This research employed four assessment metrics: KNN, DT, Naïve Bayes and RF were evaluated using the Confusion Matrix, Precision, F1-Score, Accuracy and Recall.

Table 3: Results of the Random Forest model

Models	Accuracy	Precision	Recall	F1-Score
KNN	98.24	97.99	97.91	98.00

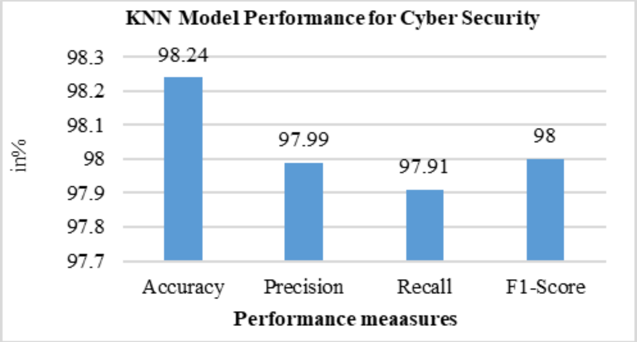

Figure 5: Bar graph of parameters performance on NSL-KDD dataset using KNN model

Table 3 shows the performance data for the K-Nearest Neighbors (KNN) model, which has a remarkable precision of 97.99%, F1-score of 98.00%, recall of 97.91%, and Accuracy of 98.24%. These measurements illustrate the model's remarkable capacity to accurately categorize data, make high-precision positive predictions, and consistently identify true positives. Figure 5 graphically illustrates these findings, displaying a balanced and near-perfect performance across all assessment parameters, with around 98% values indicating the model's overall dependability and efficacy.

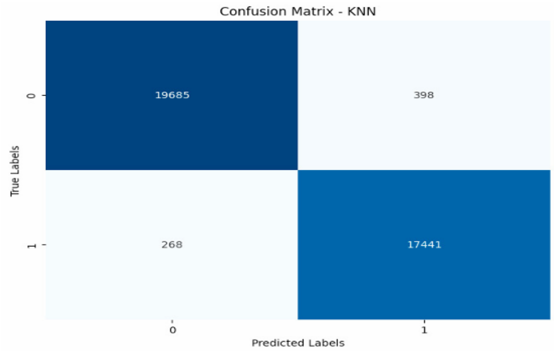

Figure 6: The confusion matrix using the KNN method on the NSL-KDD dataset

The KNN model based on the NSL-KDD for cybersecurity advancement yields the confusion matrix shown in Figure 6. There is a false label on the vertical axis and a true label on the horizontal axis in the picture. The numeral of true positive assaults, as predicted by the model, was 19,685, true negative attacks were 17,441, false positive attacks were 268, and false negative attacks were 398.

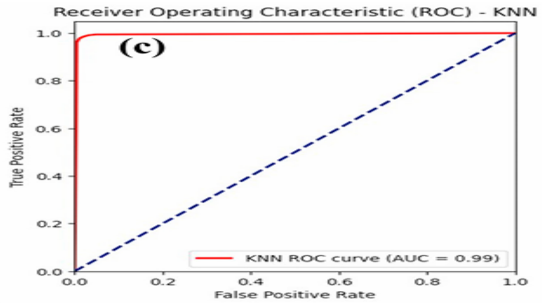

Figure 7. KNN model ROC curve on NSL-KDD dataset

Figure 7 demonstrates that the K-Nearest Neighbors (KNN) model obtained an amazing Area beneath the ROC curve (AUC) of 0.99, indicating good classification accuracy. A true positive and false positive model performance of the KNN model is graphically analyzed across different thresholds, where the ROC curve describes the consistent accuracy of the model in classifying the data points. The feature of having a high AUC value testifies to the fairly high reliability of the produced predictions that are made by the KNN model.

Table 4: Results of the different models for Detecting Cyber Attacks using the NSL-KDD dataset

Models	Accuracy	Precision	Recall	F1-Score
SVM[24]	76.05%	82.57%	80.69%	81.62%
LSTM[25]	96.63%	97.00%	97.00%	96.61%
KNN	98.24%	97.99%	97.91%	98.00%

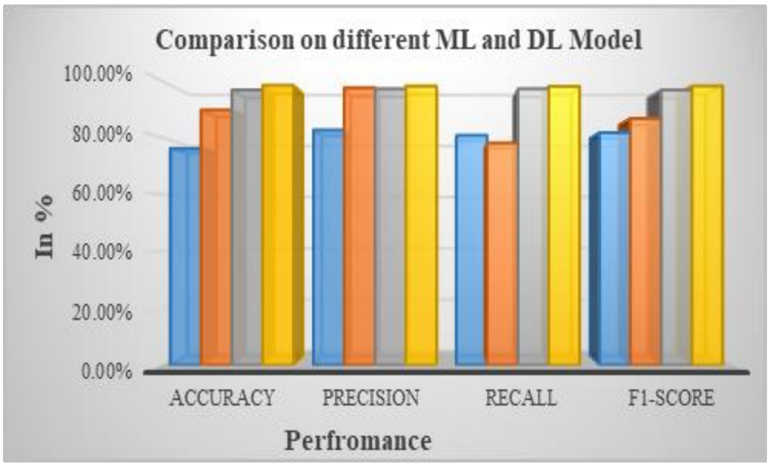

Figure 8: Comparison of ML Models for cyber security attack detection on NSL_KDD dataset

Table 4 and Figure 8 analysis provides the following insights for this thesis study. Analyzing four models (LSTM, KNN and SVM), KNN is exposed to be efficient with an , precision of 97.99%, accuracy 98.24% and, an F1-score of 98.00, recall of 97.91%. LSTM shows high accuracy, 96.63%, with reasonable recall , good precision, and F1-score having values of about 97%. SVM has moderate scores close to each other, including those such as precision, recall, and F1-score. Values. It ranges from 80% to 82% and has the lowest total accuracy for this dataset due to lower reliability.

V. CONCLUSION AND FUTURE SCOPE

Cybersecurity has become a paramount concern in the modern networked environment. Network intrusion detection systems are essential for protecting digital assets by detecting and addressing hostile actions. This finding delivers a complete analysis of the enhancement of cybersecurity in network intrusion detection, emphasizing the ML techniques to advance the accuracy and effectiveness of detecting network assaults. This Research illustrates the efficiency of ML techniques in improvement. This work analyses the NSL-KDD dataset to illustrate the efficacy of machine learning techniques in enhancing interference-finding systems. Among the analyzed models, the K-Nearest Neighbors (KNN) method showed exceptional performance with an accuracy of 98.24%, exceeding that of both SVM and LSTM. The strong findings of KNN indicate its dependability in differentiating between regular and incursion data, highlighting its potential for real-world applications. However, the paper has various limitations to overcome in future work. The dataset contains class imbalance problems and only works on binary classification; it also uses a supervised-based single ML model. Future work will use data balancing and other machine learning models and work on multiclass classification with more datasets. Future work should enhance model performance by integrating deep learning methodologies, improving generalization across various datasets, and implementing real-time threat detection capabilities to address the changing complexity of cyber threats.

REFERENCES

1. H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, and S. Shetty, “Simulation for cybersecurity: State of the art and future directions,” Journal of Cybersecurity. 2021. doi: 10.1093/cybsec/tyab005.
2. X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, and M. Sanz Rodrigo, “Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies,” IEEE Access, 2020, doi: 10.1109/ACCESS.2019.2963407.
3. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” J. Big Data, 2020, doi: 10.1186/s40537-020-00318-5.
4. 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, pp. 1–21, 2021, doi: 10.1155/2021/1302999.
5. I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” SN Computer Science. 2021. doi: 10.1007/s42979-021-00557-0.
6. S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar, “A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network,” IEEE Open J. Comput. Soc., 2021, doi: 10.1109/OJCS.2021.3050917.
7. V. V. Kumar, A. Sahoo, and F. W. Liou, “Cyber-enabled product lifecycle management: A multi-agent framework,” in Procedia Manufacturing, 2019. doi: 10.1016/j.promfg.2020.01.247.
8. R. P. Vamsi Krishna Yarlagadda, “Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity,” Eng. Int., vol. 6, no. 2, pp. 211–222, 2018.
9. M. Akhtar and T. Feng, “An overview of the applications of Artificial Intelligence in Cybersecurity,” EAI Endorsed Trans. Creat. Technol., 2021, doi: 10.4108/eai.23-11-2021.172218.
10. M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, “Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making,” Int. J. Reciprocal Symmetry Theor. Phys., vol. 5, no. 1, pp. 42–52, 2018.
11. S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2968045.
12. J. Thomas, “Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics,” J. Emerg. Technol. Innov. Res., vol. 8, no. 9, 2021.
13. R. Iftikhar and M. S. Khan, “Social media big data analytics for demand forecasting: Development and case implementation of an innovative framework,” J. Glob. Inf. Manag., 2020, doi: 10.4018/JGIM.2020010106.
14. N. D. Trung, D. T. N. Huy, and T. H. Le, “IoTs, Machine Learning (ML), AI and Digital Transformation Affects Various Industries - Principles and Cybersecurity Risks Solutions,” Webology, 2021, doi: 10.14704/WEB/V18SI04/WEB18144.
15. V. Shah, “Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats,” Rev. Esp. Doc. Cient., vol. 15, no. 4, pp. 42–66, 2021.
16. I. Sohn, “Deep belief network based intrusion detection techniques: A survey,” Expert Systems with Applications. 2021. doi: 10.1016/j.eswa.2020.114170.

17. C. Hu, J. Yan, and C. Wang, "Advanced Cyber-Physical Attack Classification with Extreme Gradient Boosting for Smart Transmission Grids," in IEEE Power and Energy Society General Meeting, 2019. doi: 10.1109/PESGM40551.2019.8973679.
18. M. Dehghani et al., "Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3051300.
19. P. Verma et al., "A novel intrusion detection approach using machine learning ensemble for iot environments," Appl. Sci., 2021, doi: 10.3390/app112110268.
20. A. A. Alsulami and S. Zein-Sabatto, "Resilient Cyber-Security Approach for Aviation Cyber-Physical Systems Protection against Sensor Spoofing Attacks," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021, 2021. doi: 10.1109/CCWC51732.2021.9376158.
21. A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2992249.
22. M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, "Improving security using SVM-based anomaly detection: issues and challenges," Soft Comput., 2021, doi: 10.1007/s00500-020-05373-x.
23. M. Koklu and I. A. Ozkan, "Multiclass classification of dry beans using computer vision and machine learning techniques," Comput. Electron. Agric., 2020, doi: 10.1016/j.compag.2020.105507.
24. A. Wang, W. Wang, H. Zhou, and J. Zhang, "Network intrusion detection algorithm combined with group convolution network and snapshot ensemble," Symmetry (Basel)., vol. 13, no. 10, pp. 1–15, 2021, doi: 10.3390/sym13101814.
25. M. Al-Imran and S. H. Ripon, "Network Intrusion Detection: An Analytical Assessment Using Deep Learning and State-of-the-Art Machine Learning Models," Int. J. Comput. Intell. Syst., vol. 14, no. 1, pp. 1–20, 2021, doi: 10.1007/s44196-021-00047-4.