Optimized Intrusion Detection System for Attack Classification Using Machine Learning and Deep Learning Techniques

Nadim Rana
Department of Computer Science, Jazan University
Jazan, 45142 Saudi Arabia
nadimrana@jazanu.edu.sa

Hamdan Alshehri*
Department of Computer Science, Jazan University
Jazan, 45142 Saudi Arabia
halshehri@jazanu.edu.sa

Mashael Ali Abdali
Department of Computer Science, Jazan University
Jazan, 45142 Saudi Arabia
mashaelabdli@gmail.com

Walaa Abdullah Madkhali
Department of Computer Science, Jazan University
Jazan, 45142 Saudi Arabia
iwalaaabdullah@gmail.com

***Abstract**:* This study addresses the escalating challenges in designing practical Intrusion Detection Systems (IDS) due to network traffic's growing intricacy and volume. A novel approach is proposed, employing a hybrid feature encoding method and utilizing Machine Learning (ML) and Deep Learning (DL) techniques for binary and multiclass network traffic classification. The system incorporates RMSPROP as an optimizer for binary classification and Adam for multiclassification. Evaluations conducted on the NSL-KDD dataset demonstrate impressive accuracy, reaching 99.28% for ML and 97.76% for DL in binary classification, 97.03% for DL and 90% for ML in detecting DoS attacks, 97.03% for DL and 90% for ML in Prop attacks, 97.03% for DL and 78% for ML in R2L attacks, and 97.03% for DL and 99.3% for ML in U2R attacks. The results underscore the effectiveness of the proposed optimized IDS, showcasing advancements in accuracy and performance through state-of-the-art ML and DL algorithms.

Keywords: Cyber-attacks, Deep learning, Intrusion Detection Systems (IDS), Machine learning

I. INTRODUCTION

Computer networks are essential in multiple areas of everyday life and industries in the modern world. People depend on desktop computers, laptops, and other internet-connected devices to reach freely accessible online information. Businesses and educational institutions create networks to help with sharing internal information. With the increasing usage of computers and online tools, maintaining network security has become a significant worry for individuals and businesses, especially regarding internet usage and protecting confidential information [1].

Intrusion detection is critical to information security, relying heavily on precisely identifying various network threats. This research explores implementing a deep learning technique for intrusion detection using recurrent neural networks (RNN-IDS). The study delves into developing an intrusion detection system utilizing machine learning and deep learning approaches. A comparative analysis of the model's performance in binary and multiclass classification tasks examines the impact of different neuron counts and learning rates. The results are compared with traditional machine learning techniques such as J48, artificial neural networks, random forests, and support vector machines. The RNN-IDS model demonstrates improved accuracy in intrusion detection, presenting a novel method that enhances the detection capabilities of intrusion detection systems. Anomaly-based detection, which uses the expected behavior of a system as a reference model, is also explored, analyzing incoming traffic to determine if it is normal or abnormal based on this model [2]. In contrast, incoming traffic is either accepted or rejected using signature-based detection, which matches it to previously set regulations. In recent years, many research publications have been created on intrusion detection systems settings [3].

Early research focused on unsupervised and supervised machine learning. Efforts have also been made to implement sophisticated applications, such as a traditional detection approach that enables the inclusion of the outcomes of several categories to enhance IDS performance significantly. The main advantage of deep learning (DL) over traditional machine learning (ML) is its ability to improve performance with larger datasets. However, DL needs help with smaller datasets, requiring large volumes of data to learn effectively. Despite its high data processing capacity, DL faces significant challenges in improving accuracy and reducing false positives as IDS datasets grow. This expansion increases the risk of misclassification and negatively impacts system performance, underscoring the need for effective feature selection to optimize classification and system efficiency [4].

II. RELATED WORK

Several researchers have utilized various datasets to train Network Intrusion Detection Systems (NIDS) algorithms aimed at identifying cybersecurity breaches. Notably, some of the most significant and well-known IDS experiments conducted between 2016 and 2024 employed different datasets to evaluate cybersecurity using machine learning techniques. The AIDS dataset is particularly effective for evaluating IDS models due to its high efficacy in identifying attacks [5].

Intrusion detection research uses the features of the NSL-KDD Cup 1999 dataset, which are divided into primary, content, traffic, and host properties. (ID). Each category analyzes ID based on the detection rate (DR) and false alarm rate. (FAR). With more than 494,020 data divided into 1,000

979-8-3503-5475-1/24/$31.00 ©2024 IEEE

clusters, K-means clustering shows the relationship between attack types and intrusion-related operations. An ANN is used to analyze the NSL-KDD dataset [6].

An association rule-mining strategy is employed to identify the two most robust attributes in the dataset, followed by classifiers to assess precision and false alarm rate (FAR). The results demonstrate that the KDD Cup 1999 dataset exhibits inferior characteristics compared to the UNSW-NB15 dataset. Additionally, three IDS benchmark datasets have been analyzed using machine learning techniques. The study leverages clustering neural network methods to distinguish between real and fake traffic. A rapid feature selection technique is also applied to identify features indicative of poor dataset quality. The findings indicate that 81.2% of intrusions and 72.9% of assaults are correctly classified by the detection rate (DR). However, further investigations have observed a decline in the effectiveness of NIDS models [7].

In another study, the variance of random variables is used to calculate the value of attributes. The examination of well-known similarity-based algorithms, such as the maximal information compression index, correlation coefficient, and most minor square regression error, shows several factors that are later added to NB and k-NN to judge the viability of the proposed method. The method ultimately outperforms existing similarity-based algorithms in terms of computational cost [8].

Feature selection methods, such as Info Gain Attribute Eval and Cfs Subset Eval are used to identify the most relevant features from a dataset, improving classification outcomes, particularly in kappa statistics, using approaches like Random Forest (RF). While some models achieve up to 99.00% accuracy in binary classification, this often reflects a bias toward dominant classes, neglecting the performance of minority classes. The study highlights the need to consider precision, false alarms, recall, F1-Score, and efficiency metrics like training time, detection time, CPU overload, and memory use, especially given the challenges posed by unbalanced classes in cybersecurity datasets and the importance of performance efficiency in high-speed, distributed environments [9].

Detecting attacks in Vehicular Ad hoc Networks (VANETs) is essential for secure communication, but traditional methods mainly focus on known attacks, leaving a gap in identifying unknown threats. To address this, a hybrid Intelligent Intrusion Detection System (IDS) is proposed, combining an Adaptive Neuro Fuzzy Inference System (ANFIS) for known attacks and a deep learning-based Unknown IDS (UIDS) using a Modified LeeNET (MLNET) architecture for unknown attacks. The system demonstrated high accuracy, precision, sensitivity, and specificity across various attack types, including DoS, Botnet, PortScan, and Brute Force, with detection times ranging from 0.95 to 1.75 seconds. Validated on the CIC-IDS 2017 dataset, the proposed IDS outperformed existing methods, highlighting its effectiveness in addressing known and novel cyber threats in VANETs [10, 11].

Similarly, two classification layers of machine learning (ML) algorithms using the NF-UQ-NIDS-v2 dataset are implemented [12]. The process includes preprocessing two sample volumes (100,000 and 10 million records) using Min Max Scaler, Label Encoder, recursive feature elimination for optimal feature selection, normalization, and hyper-parameter optimization for both classical algorithms and neural networks. In today's digital age, the surge in data is matched by a rapid increase in cyberattacks, highlighting the importance of intrusion detection systems (IDS). ML techniques are essential in this context, enabling automated analysis, pattern recognition, and intrusion classification. The results with smaller datasets showed high detection accuracy for classical algorithms like support vector machines (98.26%), decision trees (98.78%), random forests (99.07%), and K-nearest neighbors (98.16%). Neural networks, intense learning models, excelled with detection rates of 98.87% for extended short-term memory networks and 98.56% for convolutional neural networks, effectively handling large datasets and identifying hidden patterns [13].

The technique aims to enhance intrusion classification by significantly reducing the input feature set from the training data through a novel feature selection and classification merging method using support vector machines (SVM). With the growing complexity of intelligent devices and related technologies, detecting abnormal traffic has become a critical challenge in internet security. Intrusion detection systems are vital in identifying malicious activities and assessing system security by issuing alerts. This study utilizes the NSL-KDD dataset to introduce an innovative feature selection approach that improves classification accuracy by selecting only the most relevant features. The experimental results demonstrate that the proposed method achieves a classification accuracy of 88.25% using the KDD Test+ dataset and 72.42% with the KDDTest-21 dataset [14].

An intelligent intrusion detection system for network traffic employing various machine learning techniques is proposed. This system achieves higher precision than existing models and offers a robust solution for securing smart networks. As the internet rapidly expands, the rise in cyber threats underscores the importance of cybersecurity. Various attacks, such as DoS, U2R, R2L, Probe, and DNS Spoofing poses significant risks. Machine learning provides powerful tools for intrusion detection, with the potential to outperform human analysts [15].

The application of machine learning in network intrusion detection is well-explored, with numerous studies published annually. Researchers often appear keen to experiment with various machine-learning techniques to detect network intrusions. However, more detailed explanations must be given regarding the selection of specific features or the decision to use all available features in the dataset. Only a few studies focus on the feature engineering aspect of machine learning, which is crucial for optimizing model performance. This study applies machine learning algorithms, including logistic regression, Naive Bayes, K-Nearest Neighbor, and decision trees, to the NSL-KDD dataset to model intrusion detection. These algorithms are

used to identify anomalies and regular patterns, improving the accuracy of classifiers for detecting cyberattacks. The work aims to find the most effective classification and deep learning models, resulting in an advanced intrusion detection system with superior precision, offering a promising approach to protecting intelligent networks.

III. METHODS

The hypotheses for this study were as follows:

H_0: The proposed IDS method, which combines feature selection algorithms and attack characteristic features, does not enhance detection performance compared to using all features in the dataset.
H_α: The proposed IDS method, combining feature selection algorithms and attack characteristic features, does enhance detection performance compared to using all features in the dataset.

This research focused on feature formation and machine learning (ML) selection to detect network threats. It required a thorough understanding of the ML process and development approach, with a primary focus on evaluating the effectiveness of the proposed solution. The research process was carried out in the following steps:

1. Gain a comprehensive understanding of machine learning and deep learning functionality and processes.
2. Analyze and evaluate existing feature selection methods for network intrusion detection.
3. Develop and set up the ML and DL models.
4. Design and implement a new feature selection method to achieve an optimal feature subset.
5. Conduct tests, analyze the results, and document the performance of the proposed solution.

Information security is greatly aided by intrusion detection, and the fundamental technology is the ability to identify different network threats precisely. Using recurrent neural networks (RNN-IDS) as a deep learning model, we present a deep learning technique for intrusion detection in this research. We also study building an intrusion detection system based on machine learning and deep learning. Furthermore, we investigate the model's performance in binary classification and multiclass classification, and we examine the effects of the number of neurons and various learning rates on the performance of the suggested model. We contrast it with machine learning techniques, such as J48, artificial neural networks, random forests, support vector machines, etc [16, 17].

Random Forest, Support Victor Machine, Multi-Layer Perceptron (MLP), Decision Tree (J48), and Recurrent Neural Networks (RNNs) are chosen to demonstrate and compare with previous works referenced in this study. The Section is divided into research process framework, problem formulation, design and implementation, proposed model algorithm, dataset description, experiment tool, and performance metrics. Figure 1 shows the research process framework.

A. Research Process Framework

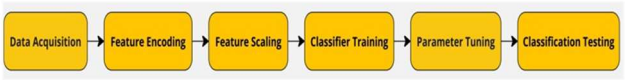

Figure 1 Research Process Framework

B. Problem Formulation

With the increasing number of cyber-attacks and data breaches, intrusion detection has become a critical aspect of computer security. Traditional intrusion detection systems rely on rule-based and signature-based approaches, which have limitations in detecting unknown and zero-day attacks. Optimized intrusion detection algorithms are necessary because of the increasing number of features in audit data and the performance failure of a human-based Intrusion Detection System (IDS) in terms of lengthy training time and classification accuracy. This project introduces an improved binary classification intrusion detection technique. The proposal is a combination of different optimization tools using machine learning and deep learning to identify malicious activities and potential threats in network traffic

C. Dataset Description

NSL-KDD is a new version data set of the KDD'99 data set. This is an effective benchmark data set to help researchers compare different intrusion detection methods.

The setting is composed of one training set and two testing sets:

- NSL-KDD Train+: The full NSL-KDD train set including attack-type labels in CSV format
- NSL-KDD Test+: The full NSL-KDD test set including attack-type labels in CSV format

Network Security Laboratory-KDD is a registered trademark. The NSL-KDD data set is an updated version of the NSL-KDD data set that was previously utilized in machine learning research. A notable benchmark data set for contrasting various intrusion detection systems is NSL-KDD [18].

- Advantage of the NSL-KDD dataset
- No redundant records in train and test datasets

D. Design and Implementation

The proposed implementation included 4 machine learning algorithms that will be used to compare with the deep learning algorithm Recurrent Neural Networks (RNNs). These are 4 Support Vector Machine learning algorithms: Random Forest, Decision Tree J48, Multi-Layer Perceptron MLP, and Recurrent Neural Networks (RNNs) deep learning algorithm. However, it is mainly applied in machine learning to classify issues. On the other hand, the random forest algorithm is an easy-to-use and adaptable machine-learning technique. Group learning is used to deal

with regression and classification issues. An overview of the Architecture of the Proposed System is shown in Figure 2.

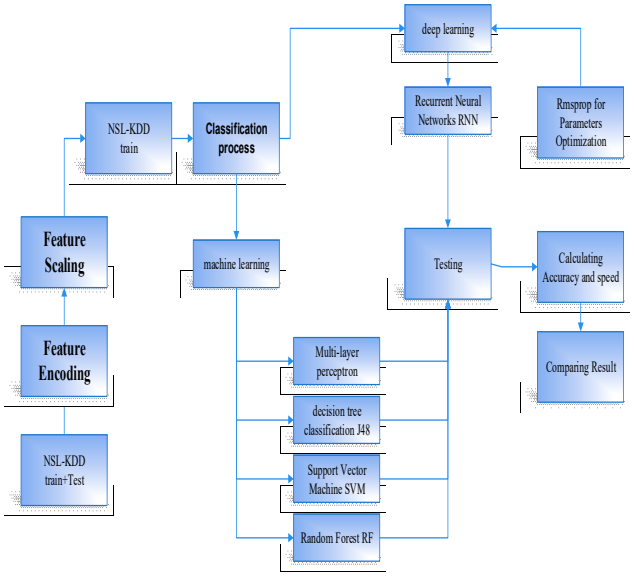

Figure 2 Overview of the Architecture of the Proposed System

IV IMPLEMENTATION TESTING AND PERFORMANCE EVALUATION

A. Data Preprocessing

Data preprocessing is a phase in the data mining and data analysis process that converts raw data into a format that computers and machine learning algorithms can understand and evaluate. Text, photos, video, and other unprocessed, real-world data could be more organized. In addition to the possibility of faults and inconsistencies, it is frequently lacking and needs a consistent design.

Machines like to process information neatly and orderly; they interpret data as 1s and 0s. Therefore, it is simple to calculate structured data like whole numbers and percentages. However, unstructured data must first be cleaned and prepared in the form of text and graphics before analysis

Step 1: Feature Encoding

i. Insert categorical features into a 2D numpy array
ii. 2. Transform categorical features into numbers using LabelEncoder ()
iii. One-Hot-Encoding for train data and test data
iv. columns are added to the main data frame
v. Convert the "label" categorical values into numerical values and put the new label column back

Step 2: Feature Scaling

i. apply the logarithmic scaling method
ii. Split the training set and testing set
iii. the value of every feature is mapped to the [0,1] range linearly

B. Testing and Performance Evaluation

There are four types of algorithms that are trained in machine learning and a deep learning algorithm and tested to detect attacks in Interta, which were mentioned earlier: Vector Machine support, Random Forest algorithms, Multi-Layer Perceptron (MLP), and Decision Tree (J48). This algorithm is used in machine learning and deep learning. Recurrent Neural Networks (RNNs).

Table 1 Precision, recall, and F1 score for Binary Classifier

*	Accuracy	Testing Phase							
		Precision			Recall			F1 Score	
	Testing	Nor	Att	WA	Nor	Att	WA	Nor	At
SVM	0.974317	99	97	98	98	99	98	99	98
RF	0.999956	99	100	98	100	98	99	99	99
MLP	0.984253	99	97	98	98	99	99	99	98
J48	1.000	99	99	99	99	99	99	99	99
RNN	0.98	100	95	98	96	100	98	98	97

As shown in Table 1, the accuracy achieved by ML methods outperforms the DL method. The MLP, Tree J48, SVM, and RF ML methods achieve accuracy ranging from 0.97 to 1.0 percent, whereas the RNN DL model achieves only 97.76%, which is less than the three ML methods. Moreover, ML algorithms also perform better in terms of loss function.

Table 2 Accuracy in Multiple classifier

Algorithm	DoS	R2L	Prob	U2R
SVM	86.88	78.2947	87.66	99.3148
MLP	90.309	77.1038	90.281	99.3864
RF	72.072	77.1038	89.6225	99.3148
J48	83.4314	77.0959	79.9044	99.3455
RNN	97.03	97.03	97.03	97.03

As shown in Table 2, the accuracy achieved by the RNN method outperformed the ML method in Multi Classification. The MLP, Tree J48, SVM, and RF ML methods achieved accuracy ranging from 0.90 to 1.0 percent, whereas the RNN DL model achieved only 97.84%, less than that of the three ML methods. Moreover, ML algorithms also perform better in terms of the loss function.

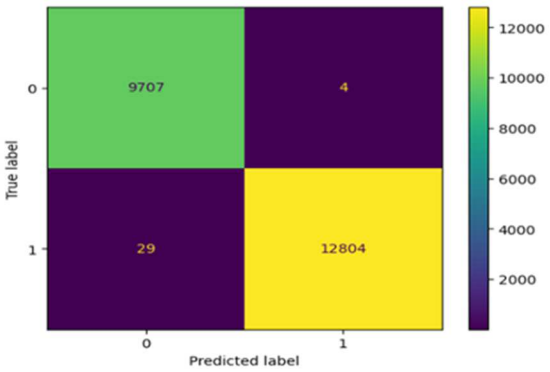

Figure 3 Random Forest Classifier

Figure 3 represents the confusion Matrix for Random Forest, which predicted significantly correctly, with a rate of 99%. It predicted that it had 12804 attacks correctly, and it predicted normality by 9707.

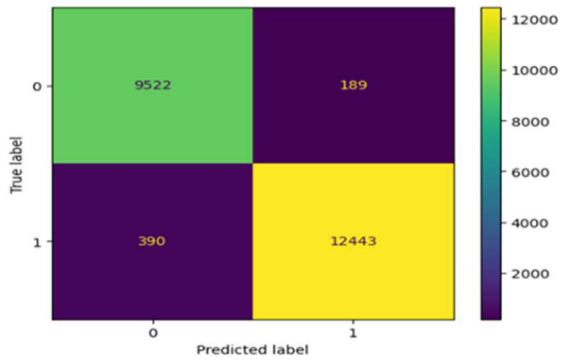

Figure 4 SVM Classifier

Figure 4 represents the confusion Matrix for the SVM Classifier, which predicted significantly correctly, with a rate of 99%. It predicted that it had 12443 attacks correctly, and it predicted normality by 9522.

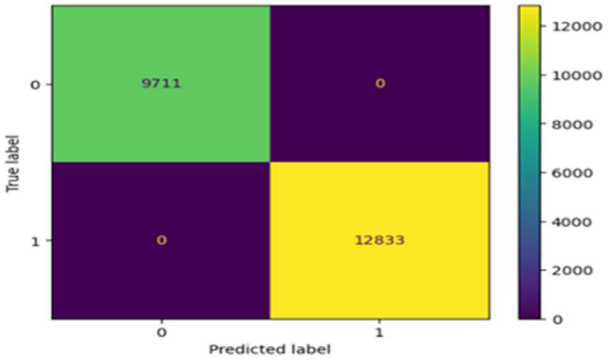

Figure 5 J48 Classifier

Figure 5 represents the confusion matrix for the J48 classifier, which was predicted to be significantly correct, with a rate of 100%. It predicted that it had 12833 attacks correctly and predicted Normally by 0711.

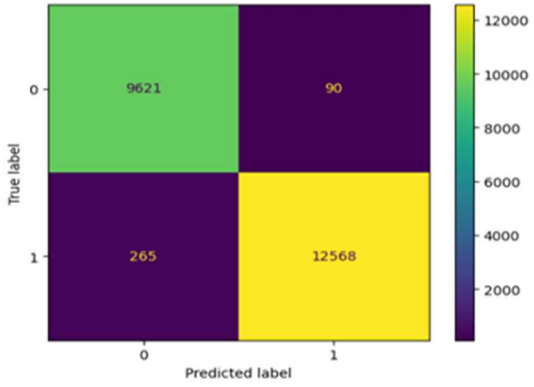

Figure 6 MLP Classifier

Figure 12 represents the confusion Matrix for the MLP Classifier, which predicted significantly correctly, with a rate of 97%. It predicted that it had 12588 attacks correctly, and it predicted normality by 9021.

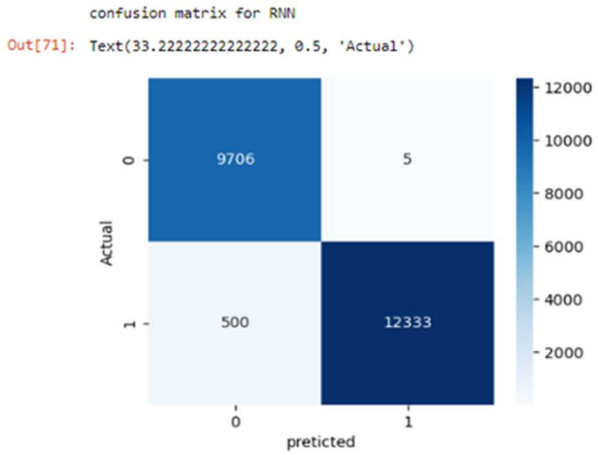

Figure 7 Confusion matrix for RNN

Figure 7 represents the confusion matrix for the RNN classifier, as it was predicted significantly correctly, with a rate of 98%. It predicted that it had 12333 attacks correctly and would normally have been predicted by 9706.

IV. COMPARATIVE RESULTS

The proposed system is evaluated using a publicly available NSL-KDD dataset. The results show that the system achieves accuracy up to 99.28% for ML and 97.76% for the DL method in detecting network intrusions in binary classifiers. We get 97.03 in DL and 90 in ML to detect a DoS attack, 97.03 in DL and 90 in ML to detect a Prop attack, 97.03 in DL and 78 in ML to detect an R2L attack, and 97.03 in DL and 99.3nin ML to detect a U2R attack consecutively.

VI. CONCLUSION

The presented work concludes that an optimal IDS solution can be developed for network attack classification using state-of-the-art ML and DL-based models. The ML and DL based IDS can significantly improve the accuracy of the attack anomalies detection. In this research, the dataset that will be used and performed is NSL-KDD. NSL-KDD is a new version data set of the KDD'99 data set. This is an adequate benchmark data set to help researchers compare different intrusion detection methods. We use machine and deep learning and find that deep learning is the best for multiple classifiers, and machine learning is the best for binary classifiers. The future direction of this research may be expected as follows:

- To experiment and develop enhanced IDS for Multi-features classification problems.
- The proposed method can be improved using advanced DL algorithms such as Long-Short-Term Memory (LSTM), generative Adversarial Networks (GAN), and Deep Belief Networks (DBN).
- Moreover, more recent training datasets with multiple classes can be utilized for various parameter improvements.

REFERENCES

[1] A. Momand, S. U. Jan, and N. Ramzan, "A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy," Journal of Sensors, vol. 2023, no. 1, p. 6048087, 2023.

[2] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," International journal of information security, vol. 22, no. 5, pp. 1125-1162, 2023.

[3] S. Einy, C. Oz, and Y. D. Navaei, "The anomaly-and signature-based IDS for network security using hybrid inference systems," Mathematical Problems in Engineering, vol. 2021, no. 1, p. 6639714, 2021.

[4] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity," Applied Sciences, vol. 13, no. 13, p. 7507, 2023.

[5] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecurity: A review," IEEE Access, vol. 10, pp. 19572-19585, 2022.

[6] D. D. Protić, "Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets," Vojnotehnički glasnik/Military Technical Courier, vol. 66, no. 3, pp. 580-596, 2018.

[7] Y. Shao, B. Liu, S. Wang, and G. Li, "A novel software defect prediction based on atomic class-association rule mining," Expert Systems with Applications, vol. 114, pp. 237-254, 2018.

[8] M. Wurzenberger, G. Höld, M. Landauer, and F. Skopik, "Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security," Computers & Security, vol. 137, p. 103631, 2024.

[9] R. Alazaidah et al., "Website phishing detection using machine learning techniques," Journal of Statistics Applications & Probability, vol. 13, no. 1, pp. 119-129, 2024.

[10] H. E. Idris and I. Hosni, "Machine Learning-Based Systems for Intrusion Detection in VANETs," in Intelligent Systems Conference, 2024: Springer, pp. 603-614.

[11] W. A. Ali, M. Roccotelli, G. Boggia, and M. P. Fanti, "Intrusion detection system for vehicular ad hoc network attacks based on machine learning techniques," Information Security Journal: A Global Perspective, pp. 1-19, 2024.

[12] A. Raza, S. Memon, M. A. Nizamani, and M. H. Shah, "Intrusion Detection System for Smart Industrial Environments with Ensemble Feature Selection and Deep Convolutional Neural Networks," Intelligent Automation & Soft Computing, vol. 39, no. 3, 2024.

[13] H. A. Gouda, M. A. Ahmed, and M. I. Roushdy, "Optimizing anomaly-based attack detection using classification machine learning," Neural Computing and Applications, vol. 36, no. 6, pp. 3239-3257, 2024.

[14] L. Tianyao, H. Huadong, and L. Run, "An Intrusion Detection Framework with Optimized Feature Selection and Classification Combination Using Support Vector Machine," in 2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI), 2023: IEEE, pp. 182-186.

[15] F. Shradha, G. Rutuja, C. Sakshi, A. Khushi, and K. Srushti, "Detection of cyber-attacks and network attacks using Machine Learning," World Journal of Advanced Engineering Technology and Sciences, vol. 12, no. 1, pp. 128-132, 2024.

[16] V. Manikandan, K. Gowsic, T. Prince, R. Umamaheswari, B. F. Ibrahim, and A. Sampathkumar, "DRCNN-IDS approach for intelligent intrusion detection system," in 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020: IEEE, pp. 1-4.

[17] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," Computer Communications, vol. 199, pp. 113-125, 2023.

[18] S. Gurung, M. K. Ghose, and A. Subedi, "Deep learning approach on network intrusion detection system using NSL-KDD dataset," International Journal of Computer Network and Information Security, vol. 11, no. 3, pp. 8-14, 2019.