Migration Letters

Volume: 21, No: S11 (2024), pp. 773-790

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Feature Reduction Based Intrusion Detection System Using Deep Learning Technique

Atiqa Abbas[1], Arslan Ali Raza[2], Asad Abbas[3], Umair Nawaz[2], Gulam Fatima[2]

Abstract

Attacks and intrusions have grown significantly due to the rapid development of networks. These attacks' detection and prevention have risen in importance as security measures. One of the key components of achieving high security in computer networks is the intrusion detection system, which is used to repel various types of attacks. The curse of dimensionality affects intrusion detection systems, resulting in less effective for incorporating resources and more complicated to run over time. The consideration of evaluating crucial features in intrusion detection system can significantly reduce the dimensions. In order to identify the useful features, this study proposes an intelligent system that first extracts features using kernel PCA (principal component analysis) as well linear discriminant analysis (LDA). A convolutional neural network (CNN) is then fed these reduced features for testing and training on NSL-KDD dataset. The extracted dataset, first normalized in order to reduce irrelevant features for the sake of quality input which ultimately classify the data into attacks and non-attacks. The standard evaluation measures; precision recall and accuracy are employed to assess the behavior of proposed system on with as well as without feature reduction. A comprehensive comparison with state of art systems has also been presented to underline the proficiency of proposed work along with the impact of feature reduction with improved QoS. Experimental evaluation revealed that our proposed optimized CNN with LDA is an effective solution as it reached to 96.1% of better accuracy with and high precision on NSL- KDD dataset, by making a reasonable margin LDA reached over Kernel Principal Component Analysis (KPCA), whereas optimized CNN with KPCA reduced the overall computational cost. We must encourage future researchers to actively participate in this research for improving and optimizing the IDSs.

Keywords: *Deep Learning, Feature Reduction, Intrusion Detection, Linear Discriminant Analysis, Machine Learning.*

1. INTRODUCTION

With the rapid growth in the IT industry, there are numerous issues started with data security. The data on the internet is not that safe enough as we consider it due to the extensive use of computer networks in numerous domains. Recent study focuses on network security as businesses understand how critical it is to safeguard their assets from loss or assault. Historically, firewalls, encryption and decryption and other methods, were used to detect intrusions. The term "first line of defense" in network security refers to these. Which makes it possible to assess the host's installed software to identify known vulnerabilities. Yet, attackers are able to sneak over them, and the initial line of security is not strong enough and adaptable to stop various intrusions or attacks. The drawback of antivirus software as a second line of protection is that it can only identify threats whose signatures are in the database. Their capacity to handle attacks that could cause them to wait many hours for the next updates is restricted. The Intrusion Detection System (IDS) is a powerful but opposing tool that captures data on actions that go against security standards. IDS take data from a system of networks and evaluate it to find component that go against accepted criteria of computer security. Three crucial qualities of an IDS are accuracy,

[1]Department of Computer Science, Institute of Southern Punjab, Multan, Pakistan.
[2]Department of Computer Science, COMSATS University Islamabad (CUI), Vehari, Pakistan.
[3]Department of Management Science, COMSATS University Islamabad (CUI), Islamabad, Pakistan.

extensibility, moreover flexibility. IDSs are used in combination with the first layer of protection to thwart intrusions from both internal and external attackers. IDS distinguish between legitimate and illegitimate users. It is a valuable tool for computer security because attackers attempt to hide their identities and launch assaults through intermediaries. Secondly, Attack detection is considerably more challenging by the constantly evolving nature of technology and approach. Hence, IDS can employ learning techniques to identify unexpected future attacks from intruders and should achieve good accuracy to counterattacks. IDS can be classified as Anomaly-based and Misuse-based categories. A hybrid IDS developed by using these both types.

Attacks that are known to the system and thus already included in the database are Misuse attacks and Signature-Based attacks. Anomalies-Based attacks are unknown and fresh for the network system. Zero-day assaults are another name for these kinds of attacks. System checks both of the attacks in Hybrid attacks category. This work cannot separate from the earlier research. To Enhance the performance of intrusion detection systems, selection of features is considered. Because, in many of the cases volume of data is quite high, so preprocessing all of them will also take quite a while. To avoid this problem and to speed up the process of data preprocessing, these features need to be reduced their sizes to increase their information value.

The question of how important a feature is in a dataset can be answered by using feature e xtraction and feature selection techniques, and categorize them according to the importance of each aspect. Classifying data traffic in networks into normal and anomaly classes is made easier with the help of these aspects. To improve intrusion detection systems' accuracy and speed, aspects that don't aid in identifying various types of attacks should be eliminated. In the process of eliminating unnecessary features, dimensionality reduction also increases other result measures such as time complexity, by putting features into categories, such as very efficient, somewhat efficient, and inefficient features. The absence of appropriate mathematical techniques makes predicting the significance of these features a challenging task. In order to figure out the strength of these features, empirical techniques might be utilized. Feature reduction helps clarify features, reduces data, boosts efficiency, and is also compatible with the use of simple classification models. After a thorough examination of the many benefits of feature reduction found in the literature—which is overflowing with research on feature selection and reduction—we present the development of an intrusion detection system that is based on feature reduction. The motivation for this work is the belief that working on every feature simultaneously for the purpose of differentiating between attack and non-attack instances is not computationally advantageous and will not improve the quality of IDS. As a result, the suggested system uses deep learning to conduct classification but first reducing the number of features present in the dataset. Normalization of dataset has been done to remove inter dependencies. The key aspect of proposed method is, it extracts features initially based on Linear discriminant Analysis (LDA) and Kernel Principal Component Analysis (KPCA), ensure that only helpful features are kept and a waste one are removed. Next, a neural network is trained on the NSL-KDD training set. The developed IDS is then test with a testing dataset, then its effectiveness is assessed using a range of statistical approaches. The study compared to other modern techniques found in the literature, and the findings are encouraging. The proposed study aims to address the following key contributions;

- Utilizing and assessing the performance of a deep learning-based classifier using the features of NSL-KDD dataset.
- Evaluating the impact of feature reduction on classification performance by employing LDA and kernel PCA.
- Analyzing the classifiers' training times and QoS for variant features of the dataset.

The rest of this paper is organized as follows: section 2 reviews the related work in this area. Section 3 presents the methodology used in this research work. Section 4 discusses the experimental results. Finally, section 5 concludes the paper and suggests future work.

2. LITERATURE REVIEW

The “dimensionality curse” of intrusion detection systems is caused by big datasets that simulate actual network data, which makes training and testing more time-consuming.

Large data sets can also result in reduced detection stability and resource consumption. It seems logical to remove data that won't help with detection before processing. As a result, a productive feature extraction and selection method that can shorten training times is produced, with increased accuracy, and protect against undetected threats. Feature reduction improves generalization, lowers computational cost and boosts learning algorithm accuracy, and makes data easier to grasp. Dimensionality reduction approaches take a high-dimensional original dataset and convert it into a new, low-dimensional dataset that preserves the original meanings of the data as much as feasible. The dimensionality curse problem is somewhat resolved by the low dimensional representation of the original data. The application of dimensionality reduction techniques to a dataset can yield multiple benefits. (i) Data storage capacity can be lowered when the number of dimensions decreases. (ii) It merely requires a shorter computation time. (iii) It is possible to eliminate noisy, redundant, and irrelevant data. (iv) The quality of the data can be raised. (v) When more dimensions are taken into account, some algorithms do not function as well. Therefore, lowering these dimensions increases the accuracy and efficiency of an algorithm. (vi) Data visualization in higher dimensions is difficult. Therefore, lowering the dimension can make it easier for us to create and analyze patterns. (vii) It increases efficiency and streamlines the classification process. Dimensionality reduction methods are normally categories as 1) feature Selection and 2) feature Extractions. Feature selection is the process of selecting a subset of the most relevant attributes from the original the collection, keeping the important details while getting rid of unnecessary or duplicate properties. However, the original features undergo transformation into a new set often of lesser dimensionality by feature extraction. The goal of this procedure is to extract the crucial information and patterns from the data so that further analysis can be done more quickly and effectively. Table I provides a descriptive summary of the methods of dimension reduction.

TABLE I. SUMMARY OF DIMENSION REDUCTION TECHNIQUES

Method	**Concepts**	**Pros**	**Cons**
Feature Extraction	Summarize dataset by creating linear combinations of features	Preserves the original, relative distance between covers latent structure, objects	Not sufficient enough in the existing of a huge number of irrelevant features
Feature Selection	A sub list of relevant features can be selected depending on defined criteria	Strong against irrelevant features	Latent structure does not cover

This paper conducts a thorough analysis of the most recent and effective techniques for data dimension reduction used in machine learning, deep learning and data mining over the last three years, as reported by researchers. Additionally, a review of each approach's details is provided, including the datasets, classifiers employed, algorithms and techniques used, and the outcomes.

Wang, et al [36] propose integrated deep intrusion detection models, namely SDAE-ELM and DBN-Softmax, to enhance computer network security. These models utilize deep neural networks, specifically Denoising AutoEncoder (SDAE) and Deep Belief Network (DBN), to address issues such as long training times and low accuracy in existing models. SDAE-ELM focuses on network intrusion detection, handling real-time data and reducing noise, while DBN-Softmax is designed for host intrusion detection, improving accuracy. The models are optimized using the ELM algorithm and Softmax classifier to overcome challenges in the fine-tuning process. Additionally, Mini-Batch gradient descent is employed for efficient parameter updates. Experimental results on various datasets demonstrate superior performance compared to traditional machine learning models. However, challenges include SDAE-ELM's less effective detection on small datasets and DBN-Softmax's prolonged training time for large datasets, hindering real-time intrusion detection. Future work aims to explore hybrid feature extraction techniques for dimensionality reduction and consider improvements to model neurons and calculation methods to enhance efficiency.

Kamil, et al [12] underscores the significance of intrusion detection systems (IDS) in network security and the increasing use of machine learning (ML) and deep learning (DL) for automated threat detection. Two detection approaches are proposed: a hybrid convolutional neural network (CNN) with Dense layers and a naïve Bayes (NB) ML technique. Evaluating these on the UNSW-NB15 Dataset, the CNN-Dense classifier outperforms ML and DL models with an impressive 99.8% accuracy. Preprocessing steps, including label encoding and normalization, are deemed essential before applying DL algorithms. The article suggests future directions, such as feature reduction techniques and integrating deep models with ML for faster classification. Overall, the proposed classifier demonstrates superior performance in accuracy, precision, recall, and F1-score metrics, affirming its efficacy in network intrusion detection. Ghani et al [7] addresses the escalating cyber threat landscape through network intrusion detection, leveraging Artificial Intelligence (AI) and Machine Learning (ML). It introduces an efficient evaluation technique for a Feedforward Neural Network (FFNN) classifier, emphasizing the use of a compact feature vector to detect network anomalies in UNSW-NB15 and NSL-KDD datasets. The results reveal that a smaller feature set outperforms larger ones in classification accuracy, avoiding computational inefficiencies associated with redundant features. The study demonstrates the efficacy of this approach in identifying unsolicited network intrusions. While the research is limited to FFNN, the authors suggest future work exploring various deep learning architectures for a comparative analysis. Planned extensions include evaluating classification accuracy for specific attack types, testing the approach with real network traffic, and integrating the model into organizational continuous integration pipelines for automated security. Azar, at al [2] mentioned security challenges in satellite-terrestrial integrated networks (STINs) and proposes four hybrid intrusion detection systems (SAT-IDSs) using machine learning (ML) and deep learning (DL). The systems leverage the sequential forward feature selection (SFS) method based on random forest (RF) to enhance detection performance. Evaluations on STIN and UNSW-NB15 datasets demonstrate improved accuracy and computational efficiency through RF-SFS feature selection. The proposed ML model, SFS-RF, achieves 90.5% accuracy on the STIN dataset and 78.52% on UNSW-NB15, while the DL model RF-SFS-GRU attains 87% and 79%, respectively. The models outperform existing literature, showcasing their efficiency in detecting various types of attacks. Future work involves constructing a new dataset with diverse satellite attacks for further model testing. Venkatesan, at al [34] used ANOVA F-Test for feature selection technique with recursive feature elimination (RFE) which extract and rank all the required features, for the purpose of building an efficient IDS, Machine Learning technique like DT, RF, SVM utilized on famous NSL-KDD dataset. RF algorithm works best with the selected features. Other ML algorithms and feature reduction techniques may be used in the future to offer an in-depth analysis with the goal of developing a more effective IDS. Since the IDS functioning can only predict known attacks, other disciplines of research and technology can potentially be used to find new attacks. Obeidat, at al [22] had done both feature reduction and feature selection to avoid irrelevant and redundant features, Principal Component analysis (PCA) BestFirst algorithm were used on NSL-KDD dataset. The following classifiers was utilized (SVM, Bayes-Net, Logistic, Naive Bayes, Part, RF, AdaBoost). Results shows that, with an accuracy rate of 80%, the Random Forest algorithm performs best. In the future, we'll study the effectiveness of better-known dimensionality reduction techniques: LDA and Kernel PCA, over distinct datasets. Goyal, at al [8] discussed the security of confidential data which is constantly under threat, CFS (Correlation Feature Selection) and Info gain was used to choose most meaningful features. The study illustrates the comparison between CLASSIFICATION ALGORITHMS: C4.5, KNN, Ripper, Naive Bayes, RM, Random Subspace and HYBRID ALGORITHMS: K-means with C4.5 and K-means with Naive Bayes and K-means with Ripper and K-means with RF. According to the results, hybrid models outperform classification approaches by a wide margin since they can detect new sorts of attacks. From all of the hybrid side, the famous K-means with C4.5 model gave highest results of 85.11%. Future studies will focus on PCA to increase detection rates.

Liu, at al [17] used a genetic algorithm for feature selection on following datasets (UNSW-NB15, NSL-KDD), using random forest (RF) classifier, the aim of the research was to build a hybrid IDS, due to the poor effectiveness of conventional signature and anomaly based IDS. As to the results, hybrid IDS perform better in multi-class classification and binary-class classification because to their low FPR and increased accuracy. In future will focus on GPU computing to shorten training time. Nagpal, at al [20] used (information gain, chi square), for feature reduction on all datasets derived from KDD99, improved SVM using Big Bang Big Crunch (BBBC) were used, the aim of the research was to overcome the raising serious global security concerns. Moving towards the results, dataset with both oversampling and under-sampling gives better results. Thirimanne, at al [33] developed a real-time IDS because several intrusion types could not be detected by the IDSs that were in place at the time. Deep neural network (DNN) has been applied data encoding and the feature scaling on famous NSL-KDD. DNN scored 81%, 96%, 70%, and 81% in terms of accuracy, precision, recall, and f1-score, respectively. By using results of this study, researchers can create dataset which displays the current network traffic patterns and identify intrusions. Rawat, at al [24] study presented IDS using machine learning techniques and deep neural networks. DL integrated framework for NIDS was presented using PCA for dimensionality reduction to drop out the less meaningful features for better detection rate and data may be kept safe from unauthorized access, DNN was utilized on NSL-KDD dataset. depending on results DNN present good accuracy. By using the proposed model to identify novel attack types, researchers can plan a direction for the future. In addition, continuous real-time model training can outperform the model training on static data. Jia, at al [11] reviewed different dimensionality reduction techniques because, curse of dimensionality can increase the cost of data storage and poor accuracy rates. Instead of using raw traffic data feature extraction and feature selection can be applied on dataset, in this way less meaningful features can be removed. Different algorithms (Based on search strategies, Heuristic search algorithms, Random search algorithms, based on evaluation criterions, non-linear feature extraction algorithms, linear feature extraction algorithms) can be applied according to the requirement. Results conclude, the first step in recognition, pattern feature extraction and selection, provides the basis for recognition training and learning. It also significantly affects recognition accuracy.

Singh, at al [28] surveyed datasets with the perspective of IDS. Following datasets (UNSW-NB15, BoT IoT, Drebin, Contagio, Genome, NSL-KDD, KDD CUP99) used on different machine learning classifiers were used DT (decision tree), SVM (support vector machine), ANN (artificial neurol network), RF (random forest), fuzzy logic. Finally, the results showed that ML approaches were capable of handling large amounts of complex data. Xu, et al [38] claimed that worldwide economic losses from cyberattacks exceed 4 trillion US dollars annually. This study used a fast parameter optimization method to minimize the number of features on the UNSW NB15 datasets, which resulted to a binary-classification accuracy of above 98%. In the future, we'll aim to apply a strategy based on behavior prediction to find attacks with a lot of the same attributes. Halim, at al [9] Considering that larger dimensionality of data has a severe effect on learning algorithms' effectiveness, the following datasets CIRA-CIC-DOHBrw 2020, UNSW-NB15 and Bot-IoT were applied to GA-based Feature Selection (GbFS) for feature selection to enhance results. The selected features were applied to a novel fitness function, and the results indicated that GbFS improved accuracy by 99.80%. Clustering is an example of an unsupervised learning strategy that can be used in the future. Oliveira, at al [23] used sentinel approach for anomalies detection through network traffic. RF, Multi-Layer Perceptron (MLP), and LSTM was employed to identify cyber-attacks. CIDDS-001 dataset was utilized. The outcome demonstrates that LSTM attain accuracy of 99.94% and f1-score of 91.66%. Future work will also include the following activities: for better understanding the model’s behavior just train LSTM for larger windows. In the second stage the refined feature engineering to improve the results. Reddy, at al [25] utilized two famous dimensionality reduction techniques (Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA)), Several of the attributes in the generated datasets may affect the results even though they are not all necessary for guiding the algorithms. By ignoring these unimportant features, the burden was reduced. The Cardiotocography (CTG) dataset was utilized in this study to test four well-known ML classifiers: Decision Tree Induction, SVM, Naive Bayes and RF. Results indicated that PCA performed better than LDA throughout the board. Moreover, applying PCA and LDA had minimal impact on the progress of algorithms, DT, and RF evaluated. In the future, high dimensionality data will be used to test the efficacy of these dimensionality reduction strategies. Additionally, similar methods can be applied to more advanced algorithms, such as convolutional neural networks and more. Li, at al [15] had done both feature selection and feature reduction respectively to avoid irrelevant and redundant features because, techniques still suffers from lack of labeled dataset, AE-IDS(Auto-Encoder) utilized on AWS dataset. Random forest algorithm was employed on the extracted features, depending on the results, The Random Forest algorithm can improve the computational cost and properly identify most attacks. Das, at al [4] used PCA for the reduction of useless features because one of the big hurdles is transforming a large amount of data into knowledgeable data. The benchmark dataset was taken from the UCI machine learning repository. Artificial Neural Network (ANN), Neuro-Fuzzy and hybrid (ANN-FR) AND (NF-FR) were used. The end result is a study into some benefits of hybrid models. Since the suggested NF-FR model outperforms the ANN, NF, and ANN-FR models in terms of efficiency, the use of the proposed method can be in image classification and document classification in future.

Kasongo, at al [13] had done both feature selection and feature reduction to avoid irrelevant and redundant features, filter-based technique using XGBoost algorithm were used on UNSW-NB15 dataset. There have been SVM, k-NN, Logistic Regression, ANN, and DT classifiers deployed. DT can use the XGBoost-based feature selection technique to increase its test accuracy for the binary classification from 88.13 to 90.85%. To implement an XGBoost-based feature selection algorithm in the future research will use famous NSL-KDD. Chen, at al [3] used CNN to design novel NIDS because traditional ML methods first need to manually select the features and has obvious limitations, so, by keeping original traffic as well as the extracted features, conventional neural network (CNN) was applied on the CICIDS2017 which resultant the better accuracy of raw traffic. For the future, researchers may put system into practical use. Riyaz, at al [26] CNN is utilized through wireless networks because the detection accuracy of current methods is insufficient. On the KDD 99 dataset, the most significant features were chosen using conditional random field and linear correlation coefficient-based feature selection (CRF-LCFS). Another method of classifying intrusions was the CNN. It is determined that proposed model obtained 98.88% of overall detection accuracy. In future, researchers can use intelligent agents for making effective decisions. Abdulhammed, at al [1] utilized Auto-Encoder and for reduction of feature on CICIDS2017 dataset for reduction of irrelevant features and to enhance results due to rapidly increasing attack rates against networked systems. The RF, Bayesian Network, LDA, and QDA classifiers were used. According to the findings, PCA is better and faster. Hence, both the binary and multi-class classification in this investigation maintained an accuracy of 99.6%. In future this trained system will be advanced to develop an IDS for online anomaly based detection. Xiao, at al [37] Created a CNN-IDS using PCA, Auto-Encoder (AE) to extract features for better detection rate. convolutional neural network (CNN) worked to encounter various problems with KDD-CUP99 dataset. According to the results, the CNN's based IDS model has higher AC, FAR, and timeliness than traditional algorithms. The issue of poor detection rates and difficult feature learning in a small number of attack categories (U2R, R2L) will be the focus of future research in this area.

In order to reduce issues like low accuracy, low detection, high false positive rate, and inability to handle new forms of intrusions, a real-time IDS was created by Dong, at al [6] For the KDD99 dataset, Flume and Flink were used for immediate cleaning and upcoming feature extraction. Neural networks were then employed to achieve a total detection rate of 94.32%. For even better results, researchers can further increase the system's functionality and performance. Shone, at al [31] used a DL model Non-symmetric Deep Auto-Encoder (NDAE) to create a network intrusion detection system by extracting features from the datasets KDD Cup99 and NSL-KDD (NIDS). The datasets in TensorFlow were further classified using Random Forest. Research results showed that the suggested model, when compared to the widely used DBN technique, offers an accuracy improvement of up to 5% and a training time reduction of up to 98.81%. Moreover, a similar level of classification accuracy was assessed on both benchmark datasets. Researchers can enhance the model in the future to defend against zero-day attacks. Ding, at al [5] used Convolutional Neural Networks (CNN), Random Forest (RF), Support Vector Machine (SVM), Deep Belief Networks (DBN), and Long Short-Term Memory Networks (LSTM) on NSL-KDD as classifiers because typical IDSs based on machine learning approaches lack dependability and accuracy. It was found that the proposed model performs better with a high DR and low FPR. Future study should focus on increasing the accuracy and DR of U2R and R2L, while also lowering the FPR of Dos. Vinayakumar, at al [35] proposed a Network Intrusion Detection System (NIDS) designed using Convolutional Neural Networks (CNN). On the KDDCup 99 dataset, the following classifiers were used: the multi-layer perceptron (MLP), CNN, CNN-recurrent neural network (CNN-RNN), CNN-long short-term memory (CNN-LSTM), and CNN-gated recurrent unit (GRU). Models are run up to 1000 epochs in each experiment, with learning rates ranging from [0.01-05]. Findings indicated that models' performance didn't much increase and that, in most cases, they produced outcomes that were comparable to CNN. Using the discussed deep learning techniques on real-time network traffic data is one potential future step. Manzoor, at al [18] features normalization was applied using (information gain, correlation method) on KDD99 dataset, The FNN was utilized, and the outcomes were encouraging. Researchers can use genetic algorithms, big bang big crunch optimization in future. Javaid, at al [10] used DL model to develop the NIDS. While developing a flexible and efficient NIDS many challenges arise. Sparse Autoencoder, Soft-Max Regression had been used on NSL-KDD dataset, because to guess unpredictable attacks less meaningful features needs to remove, Self-Taught Learning (STL) was applied for further classification, which resultant that proposed NIDS performed very well compared to previous NIDSs.

Sharma, at al [30] overviewed variants of LDA technique just to solve the small sample size (SSS) problem, feature selection, feature extraction applied on different AR, ORL datasets. Different LDA-SSS techniques used for classification with different results. According to Li, at al [16] because it is not easy to discern the attacks on less meaningful features, so, reduced the features for better results using gradually feature removal (GFR) on KDDCup99 dataset. support vector machine (SVM) was utilized for classification to detects the intrusions on the KDDCup99 dataset. Performance of gradually feature removal (GFR) was better in comparison. Mukherjee, at al [19] used Correlation Feature Selection (CFS), Info Gain, and Ration Gain for improved performance of the IDS on NSL KDD dataset, after feature selection had been done to avoid redundant and unnecessary features. According to the results, this study's suggested Feature Vitality Based Reduction Method (FVBRM) using Naive Bayes classifier achieved an overall classifier accuracy of 97.78%. In the future, the FVBRM feature selection approach will be modified to improve the results for intrusion, especially for U2R attacks. Nziga, at al [21] deployed a hybrid approach called MID-PCA, selecting features and extracting features using PCA and mRMR (Mutual Information Difference evaluation criteria) correspondingly because the KDD Cup '99 dataset has too much data for NIDS to handle. According to the results, hybrid MID-PCA exhibits improved performance and classification accuracies with reduced datasets of only 4 dimensions for BayesNet (99.77%) and 6 dimensions for J48 (99.94%). The following classifiers were used: J48(C4.5), BayesNet, PCA, and mRMR. With 12 principal components, PCA yields accuracy that is comparable. MID-PCA so performed better than PCA and mRMR. Singh, at al [29] used GDA for feature extraction because the original high dimensional database needs to be fixed up of the useless data. Intrusions were discovered using SOM and C4.5 techniques. KDDCup99 dataset were used in this study. It is found that the C4.5 classifier performs better across the board. Also, I'll present an ensemble strategy for IDS in the future, using C4.5 as an intrusion detection classifier and

GDA as a feature reduction technique. Salama, at al [27] IDS is developed to monitor any malicious behaviors in network traffic and to alert users when something suspicious found. This paper focused on hybrid IDS based on DBN- SVM model. Additionally, Features were reduced by Gain Ratio and Chi-Square for better performance. it is determined that the higher percentage of classification is shown by DBN-SVM hybrid scheme than the SVM. Kumar, at al [14] used a variety of datasets and statistical, knowledge and artificial intelligence (AI)-based methodologies. Several security concerns were focused on by employing a hybrid/ensemble strategy, which led to very accurate detection of known and unknown attacks. Future research will combine techniques for a hybrid or ensemble approach and use effective feature reduction methods for real-time traffic analysis.
The dimensionality reduction techniques using various classifiers have been presented in the literature mentioned above. The recent literature summary is included in Table II.

TABLE IV. FEATURE EXTRACTION METHODS SUMMARY

Study	Year	Source Data	Model	Approach	Evaluation
Venkatesan et al. [34]	2023	• NSL-KDD	• SVM • RF • DT	• Recursive feature elimination (RFE) • ANOVA F-Test	RF algorithm performs optimally with the selected features
Obeidat & Magableh [22]	2022	NSL-KDD	• Bayes-Net • SVM • Naive Bayes • Part • RF • Logistic • AdaBoost	• Best first • PCA	RF with accuracy of 80.5%
Goyal [8]	2022	NSL-KDD	• C4.5 • KNN • Ripper • Naïve Bayes • RF • Random Subspace • Kmeans with C4.5 • K-means with Naive Bayes • K-means with Ripper • K-means with RF	• CFS (Corelation feature Selection) + greedy search • Pearson correlation • Info gain	The C4.5 model produced the most favorable result of 85.54% with the accuracy. The Kmeans with the C4.5 method delivered super results, with accuracy of 85.11%.
Tesfahun et al. [32]	2013	NSL-KDD	Random Forest	Info Gain	Reduces the time required to develop the model and improves the detection rate for the

					minority classes.
Rawat et al. [24]	2022	NSL-KDD	DNN	PCA	Considerably better accuracy on the test set 0.793% accuracy and model fitting
Abdulhammed et al. [1]	2019	CICIDS2017	• RF • Bayesian Network • LDA • QDA	• Auto Encoder • Principal component analysis	The study showed that PCA is superior, quicker, easier to understand, and capable of reducing the data's dimensionality to as low as two components.
Xiao et al. [37]	2019	KDD-CUP99	CNN	• Auto Encoder • PCA	Results show that the CNN-IDS model outperforms standard algorithms in terms of AC, FAR, and timeliness
Li et al. [15]	2012	KDD-Cup 99	SVM	Gradually Feature Removal (GFR)	The pragmatic results indicate that the accuracy achieve is 98.6249%
Shone et al. [31]	2018	• KDD-Cup99 • NSL-KDD	RF	Non-symmetric Deep Auto-Encoder (NDAE)	Proposed model delivers up to a 5% improvement in accuracy and training time reduction of up to 98.81%
Riyaz et al. [26]	2020	KDD 99	CNN	Conditional Random Field and Linear Correlation Coefficient Feature Selection (CRF-LCFS)	Well, outcome is, proposed model provides 98.88% accuracy.

Reddy et al. [25]	2020	Cardiotocography (CTG)	• DTI • SVM • Naive Bayes Classifier • RF	• LDA • PCA	Findings indicate that PCA performs consistently better than LDA. Moreover, using PCA and LDA has little effect on how well the classifiers, DT, and RF performed.
Singh et al. [29]	2011	KDD-Cup99	• Self-Organizing Map (SOM) • C4.5	Generalized Discriminant Analysis (GDA)	For all classes (Normal, DOS, R2L, U2R, Prob), the C4.5 classifier performs better, with comparable training and testing times.
Thirimanne et al. [33]	2022	NSLKDD	DNN	• Categorical data encoding • Feature scaling	In respect to accuracy, f1-score, precision, and recall, DNN achieved 81%, 81%, 96%, and 70%.

Deep learning and intrusion detection have generally been the subject of considerable research, although more focus is still needed. Scholars devoted major time to the KDD99 and NSL-KDD datasets. Many studies concentrate on the entire feature set in its unaltered state, without any feature reduction. However, the feature extraction demonstrated that it can enhance classification performance as well as Fastly identify intrusions. In this study, we'll compare the impact of the full feature set versus extracted features on the NSL-KDD dataset. The key contrast is between the two reduction algorithms' accuracy and false positive rate as well as precision. Additionally, we analyze the training times needed for full feature set and with reduced dataset. Finding optimal strategy for delivering improved accuracy and reduced training times is the major goal.

3. **Methodology**

In Figure 1, the suggested methodology is shown. Choosing the NSL-KDD dataset, a benchmark dataset for intrusion detection systems, is the initial step. The process begins with the elimination of class-to-class interdependencies. After the data preprocessing stage, a normalized dataset is produced. The next stage uses two techniques, Kernel PCA and LDA, to extract features. It will identify the feature in a given set of feature vectors that is most helpful for learning. The classification algorithm will use these features to separate unknown cases into the "Normal" and "Anomaly" groups. Classification of traffic was conducted using machine learning reduction models, further for evaluation accuracy, and performance measures such as time and cost were considered. The subsequent sections contain the details of these modules

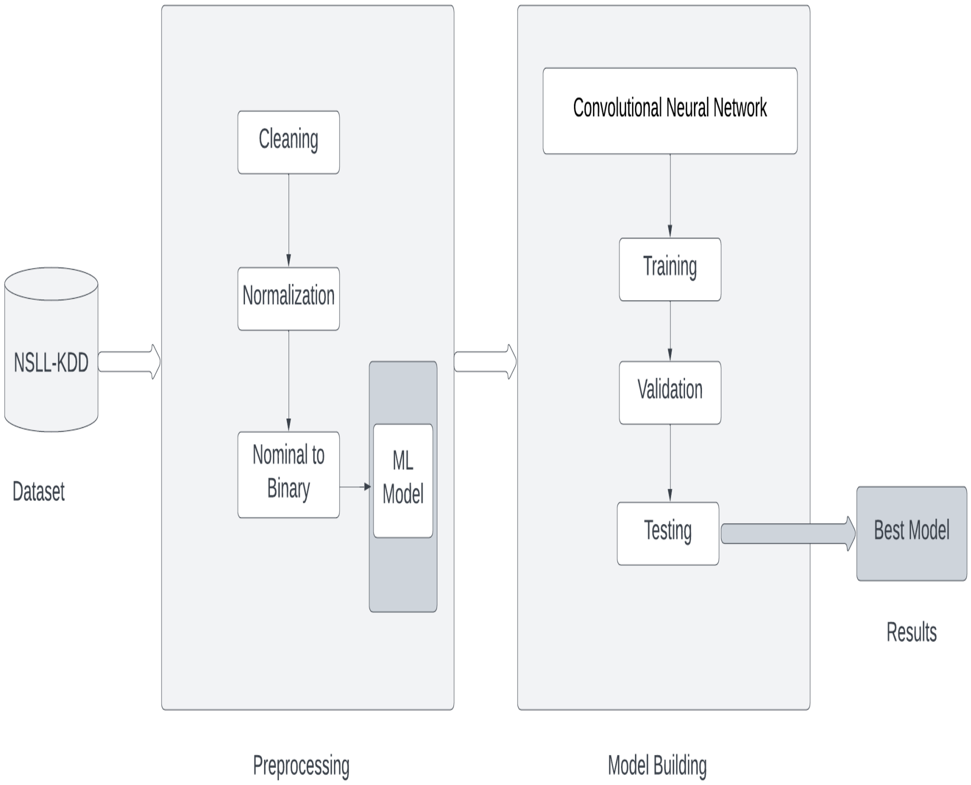

Figure 1 Diagrammatic representation of proposed method

3.1 Dataset:

The benchmark NSL-KDD dataset[1], an upgraded version of KDD99 that can be accessed from the UNB datasets repository that is being studied. It is made up of several different types of incursions that are simulated within a military network. By mimicking a normal US Air Force LAN, it produced an environment for obtaining raw TCP dump data for a network. The LAN was bombarded with several attacks and was focused like a genuine environment. A connection is a series of TCP packets that transport data to and from a source IP address to a target IP address in accordance with a predetermined protocol. The packets start and stop at a specific time interval. Dataset includes these sub-files: KDDTrain+, KDDTest+, KDDTrain+_20Percent and KDDTest-21. 41 features and 1 class label are present in the dataset with different number of instances in different files. The class indicates that coming request is one of the attacks or normal authorized requests. The targeted class of dataset is divided into two major groups; Normal and Anomaly, based on their features.

In normalization phase, the dataset transformed into Nominal to Binary form. To remove the interdependencies of features on each other, the initial step was to replace the Nan, NA or INF with 0. However, the dataset does not contain any Nan, NA or INF values. Purpose of the filter is to transform nominal/categorical data into a binary format that can easily use by ML algorithms. For each category in the original variable, a new binary variable is created to do this and assigning a value of 1 if the observation falls into that category and 0 otherwise. So, by taking each distinct category inside categorical features, binary features are created, which resultant of 122 features with 185559 instances and a target class. Each binary feature indicates whether a particular category is present or not, like One-hot encoding. After that, split dataset into testing and training datasets. For training we considered 20% which is (37111, 122) of dataset, while for testing 80% is selected which is (148448, 122) of the full feature dataset. We chose features randomly by using random state=0 for training and testing of dataset. This proportion was adopted by the various researchers in the above-mentioned literature. The last step was to reshape the independent features.

3.2 Cyber attacks:

A variety of cyberattacks that support the necessity of developing an intrusion detection system (IDS) in NSL-KDD are covered in this section.

i. **Denial of Service (DoS):**
This kind of attack is common in the realm of cybercrimes and focuses mostly on blocking the services that the system or network provides by disguising it through the use of junk requests and limiting access to just those authorized users who are there.

ii. **Probe:**
In order to launch an assault on the system, the hacker or attacker in this case tries to carefully examine all of the data and weaknesses in the system or networks that will be stored elsewhere.

iii. **Remote to Local (R2L):**
In this kind of attack, the hacker or attacker gains full access to any computer system via an illegal network. This is accomplished by periodically sending packets to the system, which will thereafter serve as the main attack vector.

iv. **User to Root (U2R):**
This kind of assault, which is common in the realm of cybercrime, involves the hacker or attacker quickly gaining access to any user with typical privilege constraints. They then take advantage of the system's administrative or root rights to carry out malicious attacks.

https://www.unb.ca/cic/datasets/nsl.html, Accessed 29-4-2021[1]

3.3 Feature Extraction:

As the dimensionality of the feature set is relatively high (41 features), we experiment with two approaches for reducing the dimensionality of the feature set:

- LDA is a statistical technique which identifies the optimal linear combination that distinguishes classes. It aims to find the projection which best calculate the separability between the classes. It more required labeled data. It is used to maximize the class separation while reducing the dimensionality. LDA aims to find a linear combination of features that best discriminates between classes. Here, by selecting the default value for n_components=None, total n_components will be minimum of no of classes-1 and no of features. After applying LDA, most corelated features extracted in linear way which captures the most discriminatory information and maximize class separation and focus on the most relevant discriminatory information. LDA component is found, and validated. This indicates that the most critical information for class discrimination can be captured by locating a linear projection of the data that optimizes the ratio of between-class variance to within-class variation.
- Kernel PCA is a widely used dimensionality reduction technique in machine learning and data analysis. Kernel PCA is an extension of PCA which is a non-linear version of it, with a kernel choice and gamma value. Kernel PCA, in contrast to PCA, uses a kernel function to project the data into a higher-dimensional space to detect non-linear correlations between the variables. Kernel PCA initially computes the kernel matrix, which represents resemblance among pairs of the complex feature space's data point. The transformed features capture intricate relationships and nonlinear patterns for enhanced feature representation, the two PC components (PC1, PC2) created using n_components=2 which holds maximum variance of features from dataset, in which features are extracted that has most impact on target class variable of dataset. PC1 is perpendicular to PC2. The top PCs holds the features with high variance and then so on, here, they represent the directions in the transformed space that best capture the intricate patterns and variations between classes as found.

3.4 Classification:

After the dataset is ready, it is input into Convolutional Neurol Network architecture model, applied by many authors as discussed in literature. A deep learning approach to evaluate and analyze information like numbers, text, photos, videos and many more using suitable layers. The transformed features passed to classifier as an input. The CNN classifier then learns to extract relevant patterns and features for accurate intrusion classification and configure appropriate activation functions, Convolutional Layers, Pooling Layers, Flatten, Dense and Fully Connected Layers. The Convolution is used to find patterns and features in input data, the pooling and activation functions are then used to lower the output's dimensionality and improve its meaning. CNNs are frequently employed in computer vision tasks such as to deal with numeric, picture segmentation, object detection, and facial recognition. The output of LDA and KPCA, is given to CNN as input, to test the classifier performance in terms of its capacity to distinguish between the normal and anomalous classes. We conduct experiments using CNN both before and after dimensionality reduction.

4 RESULTS AND EVALUATIONS

The standard evaluation measures; precision recall and accuracy are employed to assess the behavior of proposed system on with as well as without feature reduction.

4.1 Performance Evaluation:

We use the training dataset to develop the classifier and the testing dataset to test its performance in order to assess the classifiers' performance. Confusion matrix contains information actual and predicted classifications done by a classifier. The detection and identification of attack and non-attack behaviors can be generalized as follows:

True Positive (TP): the amount of attack detected when it is actually attack.
True Negative (TN): the amount of normal detected when it is actually normal.
False Positive (FP): the amount of attack detected when it is actually normal (False alarm).
False Negative (FN): the amount of normal detected when it is actually attack.

Classification accuracy is calculated on the tested data as the ratio between correctly classified samples divided by the total number of tested samples.

- **Accuracy = True Positives + True Negatives / Total**

False Positive Rate (FPR) is calculated as the number of false positives divided by the total number of true negatives and false positives.

- **False Positive Rate= False Positive / False Positive + True Negative**

Precision is calculated as the ratio of true positives to the sum of true positives and false positives. Higher precision values suggest a lower rate of false positives in the model's predictions.

- **Precision=True Positives / True Positive + False Positive**

4.2 Evaluation and Findings

The results of the tests are discussed in this section; first, we present the results of classification before performing dimensionality reduction. After that, we provide the classification result using LDA. The impact of the KPCA method on classification performance is then examined.

a) EXPERIMENT 1: Analysis using full feature set

We build the classifier in this experiment using the deep learning algorithms which were previously explained. This is achieved by utilizing the training dataset. We make use of all 41 of the features. The model is evaluated using the testing dataset after it has been built. The accuracy, FPR, and precision results are shown in the table.

TABLE I. RESULTS USING FULL FEATURE SET

Model	Accuracy	False Positive Rate (FPR)	Precision
0.9554	0.009	0.980	0.9554

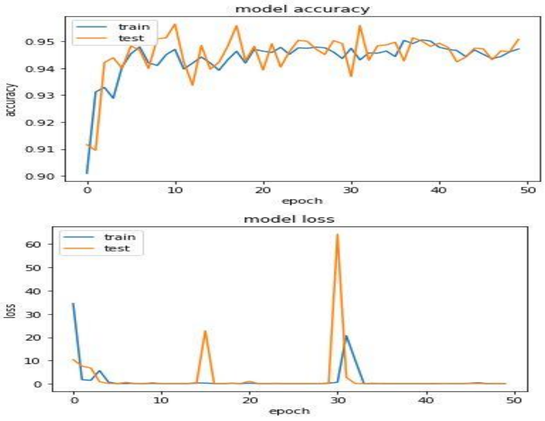

Fig. 2. PROGRESS OF FULL FETURE SET

b) **Experiment 2: Extracted features after LDA**

In this experiment, we begin by employing LDA to reduce the dataset, and then we test how well the classification algorithms perform in the feature space that has been reduced. This table makes it obvious it has the highest reported accuracy.

TABLE II. RESULTS AFTER LDA

Model	Accuracy	False Positive Rate (FPR)	Precision
CNN-LDA	0.9616	0.005	0.994

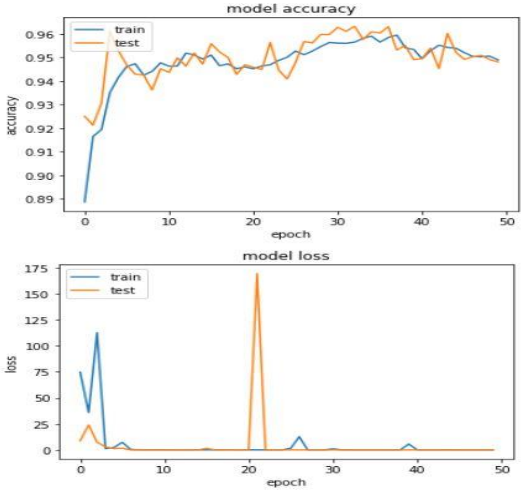

Fig. 2. PROGRESS OF LDA

c) **Experiment 3: After KPCA Feature Extraction**

KPCA is also employed for reduction of dataset, and although the results are not better than with the prior model, but the time complexity of this model is still lower than other models. The KPCA's classification performance, however, has not gotten better.

TABLE III. RESULTS AFTER KPCA

Model	Accuracy	False Positive Rate (FPR)	Precision

CNN-KPCA	0.9130	0.071	0.926

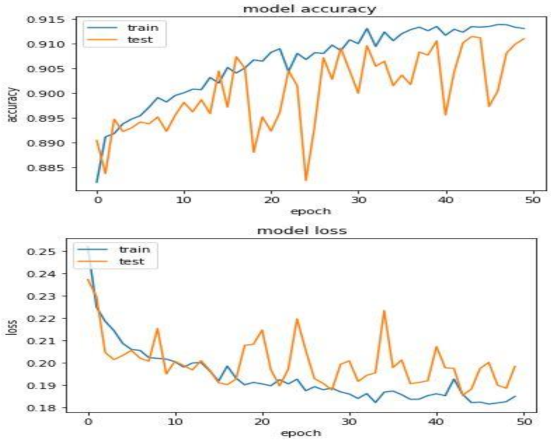

Fig. 3. PROGRESS OF KPCA

We further demonstrate the results, in Fig. 4. An illustration of the training time logs for both the derived datasets and the original full feature set, to better understand which algorithm takes more computational cost. An identical machine was used for each experiment.

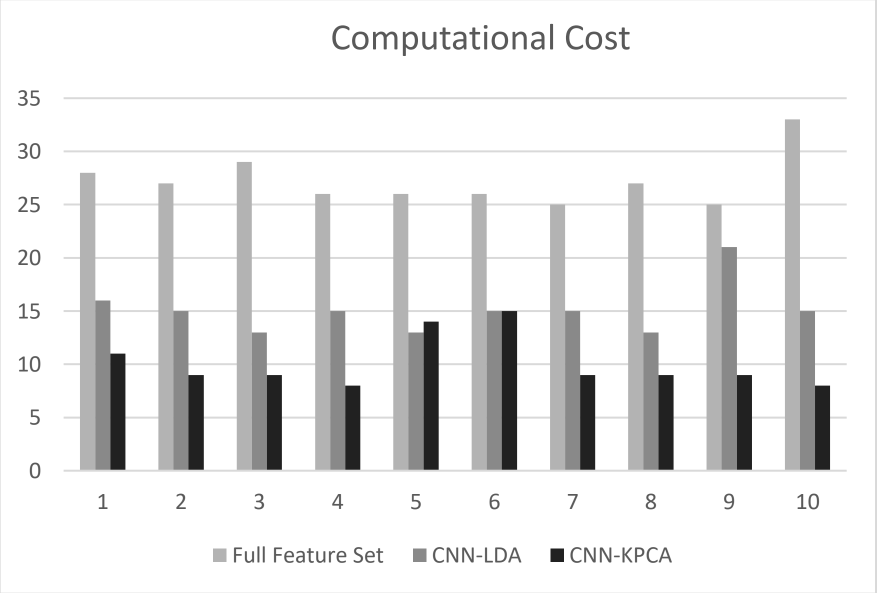

Fig. 4. COST COMPARIONS FOR ALL MODELS

Overall, feature reduction minimizes the duration of training time for both algorithms rather than full feature set. Moreover, we can note that, K-PCA performs best in term of computational cost. This experiment runs on 50 epochs, but the computational cost presented in this graph is on ten notable epochs. In summarizing the findings, we may say that LDA-CNN model performs best with reduced features set, as it gives best results with 96% accuracy and improved QoS. After that better result provided by CNN using full feature set with 95% of accuracy but utilized more computational cost in term of time and loss, the algorithm that didn’t performs well on reduced feature set is KPCA as it effects QoS with less accuracy of 91% but it saves more computational cost. On the NSL-KDD dataset, algorithms can be useful in improving classifier performance, with the range of improvements employing LDA considerably stronger over KPCA. It is emphasized that feature selection provides a significantly better result than using CNN on the full dataset while also cutting down on training time. However, although having similar highest accuracy rates to the KPCA algorithm, LDA requires more training time.

4. CONCLUSION AND FUTURE WORK

The goal of this analysis incorporates a CNN-based Model (CNN) using benchmark Dataset (NSL-KDD). The findings demonstrate that, in terms of accuracy, FPR, and precision classifier performs best using LDA as a feature reduction model with 97% results. Additionally, we produce accuracy and FPR graphs for each case, showing that the training times are the most consistent over the course of each period iteration. Proposed model overcomes the problem of time complexity. In the long term, these techniques can also be implemented using some different dataset, we might also perform some other feature selection methods with deep learning to increase the QoS.

REFERENCES

[1] Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics, 8(3), 322.

[2] Azar, A. T., Shehab, E., Mattar, A. M., Hameed, I. A., & Elsaid, S. A. (2023). Deep Learning Based Hybrid Intrusion Detection Systems to protect Satellite Networks. Journal of Network and Systems Management, 31(4), 82.

[3] Chen, L., Kuang, X., Xu, A., Suo, S., & Yang, Y. (2020, December). A novel network intrusion detection system based on CNN. In 2020 eighth international conference on advanced cloud and big data (CBD) (pp. 243-247). IEEE.

[4] Das, H., Naik, B., & Behera, H. S. (2020). A hybrid neuro-fuzzy and feature reduction model for classification. Advances in Fuzzy Systems, 2020, 1-15.

[5] Ding, Y., & Zhai, Y. (2018, December). Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In Proceedings of the 2018 2nd International conference on computer science and artificial intelligence (pp. 81-85).

[6] Dong, Y., Wang, R., & He, J. (2019, October). Real-time network intrusion detection system based on deep learning. In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS) (pp. 1-4). IEEE.

[7] Ghani, H., Virdee, B., & Salekzamankhani, S. (2023). A deep learning approach for network intrusion detection using a small features vector. Journal of Cybersecurity and Privacy, 3(3), 451-463.

[8] Goyal, J. (2023). Model Based Intrusion Detection using Data Mining Techniques with Feature Reduction. Authorea Preprints.

[9] Halim, Z., Yousaf, M. N., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., ... & Hanif, M. (2021). An effective genetic algorithm-based feature selection method for intrusion detection systems. Computers & Security, 110, 102448.

[10] Javaid, A., Niyaz, Q., Sun, W., &Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (pp. 21-26).

[11] Jia, W., Sun, M., Lian, J., & Hou, S. (2022). Feature dimensionality reduction: a review. Complex & Intelligent Systems, 1-31.

[12] Kamil, W. F., & Mohammed, I. J. (2023). Deep learning model for intrusion detection system utilizing convolution neural network. Open Engineering, 13(1), 20220403.

[13] Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 7, 1-20.

[14] Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review, 34(4), 369-387.

[15] Li, X., Chen, W., Zhang, Q., & Wu, L. (2020). Building auto-encoder intrusion detection system based on random forest feature selection. Computers & Security, 95, 101851.

[16] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert systems with applications, 39(1), 424-430.

[17] Liu, Z., & Shi, Y. (2022). A hybrid IDS using GA-based feature selection method and random forest. Int. J. Mach. Learn. Comput, 12(2), 43-50.

[18] Manzoor, I., & Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. Expert Systems with Applications, 88, 249-257.

[19] Mukherjee, S., & Sharma, N. (2012). Intrusion detection using naive Bayes classifier with feature reduction. Procedia Technology, 4, 119-128.

[20] Nagpal, M., Kaushal, M., & Sharma, A. (2022). A Feature Reduced Intrusion Detection System with Optimized SVM Using Big Bang Big Crunch Optimization. Wireless Personal Communications, 122(2), 1939-1965.

[21] Nziga, J. P., & Cannady, J. (2012, September). Minimal dataset for Network Intrusion Detection Systems via MID-PCA: A hybrid approach. In 2012 6th IEEE International Conference Intelligent Systems (pp. 453-460). IEEE.

[22] Obeidat, I., & Magableh, K. (2022, March). Dimensionality Reduction and Supervised Learning for Intrusion Detection. In 2022 8th International Conference on Information Management (ICIM) (pp. 86-91). IEEE.

[23] Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences, 11(4), 1674.

[24] Rawat, S., Srinivasan, A., Ravi, V., & Ghosh, U. (2022). Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. Internet Technology Letters, 5(1), e232.

[25] Reddy, G. T., Reddy, M. P. K., Lakshmanna, K., Kaluri, R., Rajput, D. S., Srivastava, G., & Baker, T. (2020). Analysis of dimensionality reduction techniques on big data. Ieee Access, 8, 54776-54788.

[26] Riyaz, B., & Ganapathy, S. (2020). A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft Computing, 24, 17265-17278.

[27] Salama, M. A., Eid, H. F., Ramadan, R. A., Darwish, A., &Hassanien, A. E. (2011). Hybrid intelligent intrusion detection scheme. In Soft computing in industrial applications (pp. 293-303). Springer, Berlin, Heidelberg.

[28] Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. International Journal of Computers and Applications, 44(7), 659-669.

[29] Singh, S., Silakari, S., & Patel, R. (2011). An efficient feature reduction technique for intrusion detection system. In 2009 International Conference on Machine Learning and Computing. Singapore (pp. 147-153).

[30] Sharma, A., &Paliwal, K. K. (2015). Linear discriminant analysis for the small sample size problem: an overview. International Journal of Machine Learning and Cybernetics, 6(3), 443-454.

[31] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[32] Tesfahun, A., & Bhaskari, D. L. (2013, November). Intrusion detection using random forests classifier with SMOTE and feature reduction. In 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (pp. 127-132). IEEE.

[33] Thirimanne, S. P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., & Hewage, C. (2022). Deep neural network based real-time intrusion detection system. SN Computer Science, 3(2), 145.

[34] Venkatesan, S. (2023). Design an Intrusion Detection System based on Feature Selection Using ML Algorithms. Mathematical Statistician and Engineering Applications, 72(1), 702-710.

[35] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1222-1228). IEEE.

[36] Wang, Z., Liu, Y., He, D., & Chan, S. (2021). Intrusion detection methods based on integrated deep learning model. computers & security, 103, 102177.

[37] Xiao, Y., Xing, C., Zhang, T., & Zhao, Z. (2019). An intrusion detection model based on feature reduction and convolutional neural networks. IEEE Access, 7, 42210-42219.

[38] Xu, Z., & Liu, M. (2021, July). An Intrusion Detection Method based on PCA and ResNet. In 2021 3rd International Conference on Applied Machine Learning (ICAML) (pp. 52-56). IEEE.