Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Enhancing The Performance of Intrusion Detection Using CNN And Reduction Techniques

Inbithaq A. Shakir[a], Hazem M. El-Bakry [b], Ahmed A. Al-fetouh Saleh [a,b,*]

[a] Department of Information Systems, Faculty of Computers & Information,, Mansoura University, Egypt .Email: inbethaqahmed_2020@yahoo.com

[b] Department of Information Systems, Faculty of Computers & Information, Mansoura University, Egypt .Email: helbakry5@yahoo.com

[a,b]Department of Information Systems, Faculty of Computers & Information, Mansoura University, Egypt

E-mail: elfetouh@mans.edu.eg

ARTICLE INFO

Article history:
Received: 25 /03/2023
Rrevised form: 03 /05/2023
Accepted : 04 /05/2023
Available online: 30 /06/2023

Keywords:

Artificial Intelligent

CNN Algorithm

PCA

Deep Learning

Intrusion Detection UNSW-NB15

ABSTRACT

There have been several security solutions based on artificial intelligence (AI), such as intrusion detection systems (IDS),cyberattacks are increasing because big data is increasing by using the internet on all sides of life, therefore, unbalanced data poses a serious problem in intrusion detection systems. The proposed detection system that is based on deep learning Convolutional Neural Network(CNN)partitions data into training and testing., Creating the classifier model for the Principal Component Analysis (PCA)technique of reducing features, is required for the development of intelligent analytic tools that need data pre-treatments and deep learning algorithm-performance enhancement. The UNSW-NB15 data set is used According to experimental findings, We employed a number of evaluation tools to assess the proposed NIDCNN strategy relying on the UNSW-NB15 data set that takes 30% of it for testing and after processing this part of the data became used to evaluate the proposed system. Measures such as a classifier's F-Score, precision, and sensitivity (Recall) are evaluated. Classifier performs better than the other approaches at determining if the data stream is normal or malicious. which is used to assess deep learning's effectiveness, the suggested model results from a high level of accuracy. The experimental findings demonstrate the suggested system's ability to accelerate the intrusion detection process while reducing memory and CPU usage. Experimental results prove the theoretical considerations.Because the UNSW-NB15 data set contains a wide range of patterns that accurately represent contemporary real network traffic, New NIDS algorithms can therefore be assessed using it.

MSC..

https://doi.org/10.29304/jqcm.2023.15.2.1234

1.Introduction

Intrusion Detection System is a useful technique for computer networks' defense-in-depth. Network-based IDS scans network traffic for known or prospective harmful actions and issues a warning anytime anything suspicious is found. For the creation of IDS, neural networks, fuzzy logic, and Support Vector Machines (SVM) consider having been machine learning [1].To enhance classification performance for the training data. Some features in the high-dimensional feature space problem might be unnecessary

*Corresponding author

Email addresses:

Communicated by 'sub etitor'

or unimportant. It is crucial to eliminate these unnecessary or redundant characteristics because doing so could damage classifier performance. Finding a subset of characteristics that will increase prediction accuracy or reduce the size of the structure without significantly lowering the classifier's built-in prediction accuracy is known as feature selection[2].reduce dimensionality by providing a linear map of n-dimensional feature space to a reduced m-dimensional feature space. estimate the UNSW-NB15 dataset and propose an anomaly intrusion detection system relying on deep learning CNN, where PCA is applied for feature reduction, examining the effectiveness of this suggested system. convolutional neural network (CNN), a regularized multi-layer perceptron, is a component of the proposed deep learning model[3,4]. Custom -hyper parameters for convolution operations include filter size, filter counts, and output matrix generation strides. While the input propagates through several convolutional layers, jointed input padding is used to accommodate diminishing tensor dimensions [5]. In order to down sample or lower the feature dimensions across the layers, the pooling layer is employed between subsequent convolutional layers. classification output layer is next mentioned, followed by a fully linked layer with regularization. Network intrusion detection systems that incorporate pertinent elements and typical cyber problems and weaknesses, employing the most recent dataset of simulated web traffic. The proposed deep learning classification architecture with the PCA technique exhibited considerable improvements to classification models when compared to the results of similar deep learning-CNN-based network IDSs[6,7]. A method for improving the definition of patterns belonging to different classes is feature reduction (RF), which involves deleting unnecessary and redundant characteristics and selecting the best subset of features[7,12]. In this study, reduction features were created using PCA reduce approaches.

The main contributions of the study can be summed up as follows:

• By fusing IDS strategies and deep learning techniques, this study evaluates the state of an IDS network.

• Deep learning-based intrusion detection systems should become more predictable. Neural Convolutional Networks

• Use CNN to process a dataset by extracting characteristics in different ways, predicting upcoming incursions, and obtaining more precise detection results.

• To increase efficiency, enhance the suggested model using the PCA feature reduction methods.

• Assess and contrast the proposed NIDSCNN using the datasets from UNSW-15.

The paper's structure includes. The following contains information on intrusion detection system research: previous works in section 2. Section 3's background information. Provide a proposed model in section 4. Section 5 contains experimental findings and discussions. Finally, section 6 provides a conclusion.

2. Previous works

R. Almarshdi et al. [8] Using the UNSW-NB15 dataset, construct an (IDS) architecture that relies on a (CNN) and Long Short-Term Memory (LSTM) model combination to find security breaches in IoT. A balanced and unbalanced dataset was used to compare the suggested model to the CNN model. The model performed with an accuracy of 92.10%.

M. Hassan et al. [9] using a crossbred deep learning technique that effectively detects network intrusions using a weight decrease long –short term memory (WDLSTM) and a (CNN) network. to extract relevant features from IDS vast data to prevent overfitting on recurrent connections. results obtained 97.1% accuracy on the sizable UNSW-NB15 dataset.

P. Wu and H. Guo [10] coordinate Recurrent Neural Networks(RNN) and CNN so that they can acquire the inputs at a comparable level of detail. To speed up learning, batch normalization is also incorporated into the architecture The UNSW-NB15 sets, have accuracy ratings of 84.98%.

M. Azizjon et al. [11] create a machine-learning model for the Standardized regression on the 1D-CNN, by serializing Transmission Control Protocol / Internet Protocol (TCP/IP) packets through an identified time. Testing using the UNSW NB15 IDS dataset, and the findings show detection performance of 89.93%,

A.Aleesa et al.[12] IDS based on Deep Learning (DL) algorithms including Artificial neural network (ANN), Deep Neural Networks (DNN), and Recurrent Neural Networks (RNN) has been proposed. To find abnormal patterns, the UNSW-NB15 the suggested deep learning techniques achieved accuracy in the multi-class category of 99.59% and accuracy in the binary classification of 99.26%.

L. Ashiku et al. [13] deep learning techniques for developing a network-based (IDS) that can recognize and classify threats. effectiveness of the model was demonstrated using the UNSW-NB15 dataset. results revealed a performance accuracy of 95.6%. this technique requires massive data to perform better.

M. Hooshmand et al. [14] constructed a base for a 1D-CNN framework. The proposed approach initially organizes NetFlow data for the (TCP), User Datagram Protocol (UDP), and OTHER protocols before processing each group independently. , The accuracy rate is 76.3% using the UNSWNB15 dataset.

In all related works, I focused on accuracy at the end of each work, in order to compare it with the model proposed in my work, and to indicate that the accuracy I obtained was higher than in previous works.

3.Theortical Background

3.1.deep learning CNN techniques

Designing (NIDS) using several supervised deep-learning classifiers , this study explores how well classifiers perform when the PCA technique is used to reduce the dimensions and decrease the time required to detect assaults. The weights are shared locally in convolutional neural networks (CNN), which means that they are applied consistently across the input[15]. Together, the weights coupled to the same output device form a filter. (1)A CNN layer is made up of the input convolutional with a number of trainable filters to extract local features. (2) A point-wise non-linearity that allows deep architectures to learn non-linear representations of the input data, similar to the logistic function. (3) a pooling operator that combines the statistics of the features at neighbouring locations to reduce computational costs as a result of the image's decreasing spatial size. Adding an output layer with all connections after the final convolutional layer [16].

3.2.dimensionality reduction techniques

The dimensionality curse problem is typically overcome by the initial data's low-dimensional data representation, which also makes analysis, processing, and visualization simple. benefits of applying dimensionality reduction techniques to a dataset[17].

1- diminution of the dimensions number and the data storage space size. 2- The computation takes less time. 3- It is possible to eliminate redundant, noisy, and irrelevant data. 4- It's possible to improve data

quality.5-Increases accuracy and facilitates the efficient operation of an algorithm. 6- Enable data visualization 7- It streamlines classification and boosts output as well [18,19].

With the constant production of data at an ever-increasing rate, feature selection (FS) is regarded as a crucial strategy since it allows for the effective reduction of redundancy, the elimination of unneeded data, and an improvement in the readability of findings. Furthermore, To enhance the competence of data processing and storage, feature extraction, determining the most distinct, perceptive, and condensed set of attributes are solved.

3.2.1.principal component analysis

Unsupervised learning techniques like the PCA reduce the dimensionality of data. The PCA, a dimensionality reduction technique created by Karl Pearson in 1901, is commonly used to divide the features of large data sets into smaller features that contain the most data [20]. PCA is frequently used to analyze data in an enormous range of fields. reviewed the PCA method for a number of theoretical and practical aspects [21].One of PCA's benefits is that it can eliminate duplicate features in a data set. (2) Useful data is gathered to explain the high contrast and best resolution. (3) It improves the data's display. (4) It makes computations simpler and more effective. this tool enables the analysis of datasets that could include multi-collinearity, missing values, categorical data, and erroneous measurements. The objective is to identify the key information in the data and express it as a collection of summary indices known as primary components. deep learning algorithms and using PCA as a Dimensionality Reduction(DR) Method for classification is one of the most crucial uses [22,23]

some undesired features may arise. In order to address these issues, begin calibrating the variants. Each data value is centered and divided into segments by the standard deviation from the vector measurements [24] when units change in one or more variables, according to the PCA (variance) standard that is based on the units of measure Computers based on a matrix covariance can change.since the covariance matrix of the standard dataset is practically the correlation matrix of the original data set so PCA considers the correlation matrix for standard data. matrix's eigenvectors used to describe the linear combinations to standard variables [25]. These PCAs are not primarily connected with the covariance matrix's previously established PCAs [26] the matrix of correlation is directly proportional to the number of variables employed in the analysis. therefore PCAs are the best option because they are invariant to linear changes in measurement units. The covariance of the PCA matrix is significant. Because to the similarity of the variances in the original component, a PCA correlation matrix is produced. A portion of the overall variance is represented by the first two matrix PCs. For different datasets, differences may be more significant [27,28].

The stages of the PCA are shown [29,30]:

- X represent a PCA input matrix with just an n-vector and an m-dimensional data collection.
- Using Eq,(1), determine the average data (X) for every dimension[30]:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad (1)$$

n samples number,

X_i item values i.

- Use the given Eq. (2) to determine the covariance matrix (C x)[30]:

$$C_x = 1/n-1 \sum_{i=1}^{n}(X_i - \bar{X})(X_i - \bar{X})^T \qquad (2)$$

- Using Eq. (3), determine the eigen-values , eigen-vectors (v m) of the covariance matrix[30]: eigen-values denoted by m

eigen-vectors denoted by v m

$$C_x v_m = \lambda_m v_m \quad (3)$$

- The eigenvalues put in descending order..
- A set of eigenvectors known as a principal component (PC) corresponds to the arranged eigenvalues from step 5.

4-Proposed Classification Model

the structure suggested on this side. The major steps are necessary to accomplish the goals. Each phase is covered in detail in the following subsections, The first step in data preparation is standardization. Second, PCA techniques lower the number of features required during the classification phase and determine which ones are most important. With the help of the suggested (NIDCNN) model, the third stage estimate the network data flow is normal or abnormal. In the end, a variety of metrics were used to assess the results of the proposed model.

First Stage: Load UNSW-NB15 dataset

to create the arriving network packets for the UNSW-NB 15 dataset in the UNSW Canberra Cyber Range Lab, IXIA PerfectStorm program was used to provide a blend of real-world contemporary daily operations and synthetic current attack,characteristics. The tcpdump application was used to record 100 GB of unprocessed traffic (e.g., Pcap files). There are nine types of attacks in this dataset, by Using 12 algorithms, the Argus and Bro-IDS tools are utilized to generate 49 characteristics with the class label. The UNSW-distinctive traits NB15 The features are described in a CSV file, There are a total of 540,044 records in the four CSV files UNSW-NB15 (1,2,3,4.csv UNSW-NB15) in the four CSV files.

By separating this data into a training set of 175.341 records and a testing set of 82,332 files for the UNSW NB15.csv.

Second stage : UNSW-NB15 Dataset division

The Hold-out-validation method was used to guarantee accurate generalization and avoid overtraining. 70% of the sets are for training, while 30% are for testing.the UNSW-NB15 dataset was divided into two subsets. The details of this approach are explained as follow:

Algorithm 1 The "Dataset division"

- UNSW-NB15 dataset as inputs
- Show the values by splitting the dataset into practice and examination sets (70/30).
- start
- Sets of model parameter values for evaluation are explained.
- any group coefficient resulting from all iterations of repetition and sampling
- Conclusion: Apply the model to the remaining data after removing a particular sample.

- Learn about the recalcitrant samples.
- pause for
- It is important to assess how hold-out estimates typically perform.
- pause for
- Choose the best possible combination of parameters.
- Using the idealistic parameter group, fit the final model to the entire set of workout data.
- End.

Third stage: Preprocessing UNSW-NB15 Dataset

Preprocessing, , seeks to transform the raw dataset into a straightforward and effective format. the primary goal of creating a dataset suitable for deep learning algorithms is to ensure its reliability. In this case, the conventional scaler strategy is used to finish this level. according to algorithm (2), When the data had been separated in the previous stage, it was employed as a preprocessing. Both situations include this procedure (training and testing).

Algorithm 2

Input: Division dataset

Output: Standardized data

- start
- Find $\text{Mean}(\bar{X}) = \frac{\sum_{i=1}^{n} X_i}{n}$ then set the result as μ.
- Find $\text{Variance} = \frac{\sum_{i=1}^{n} (X_i - \bar{X})^2}{n-1}$
- Find standard deviation $(\text{SD}) = \sqrt{\frac{\sum_{i=1}^{n} (X_i - \bar{X})^2}{n-1}}$, represent result as σ.
- Find stander scaler $Z_{Scaled} = \frac{(X-\mu)}{\sigma}$
- End

Forth Stage: Reduce features firstly using PCA,

Algorithm (3)

Input: Standardized data (SD)

Output: Reduced features (RF)

- start

- Establish a data matrices with each of the values for the parameters in the columns and then each row represents a distinct item in the row.
- Compute covariance matrix using Eq. $C_x = 1/n-1 \sum_{i=1}^{n}(X_i - \bar{X})(X_i - \bar{X})^T$.
- Calculate covariance matrix's eigenvalues and eigenvectors $C_x = 1/n-1 \sum_{i=1}^{n}(X_i - \bar{X})(X_i - \bar{X})^T$ and $C_x v_m = \lambda_m v_m$
- Using eigenvalues to reduce the dimension data
- Return (Reduced Features)
- finish

Fifth Stage: Create a 27-layer NIDCNN classification model.

The proposed categorization model was demonstrated in diagram (1) and algorithm (4).

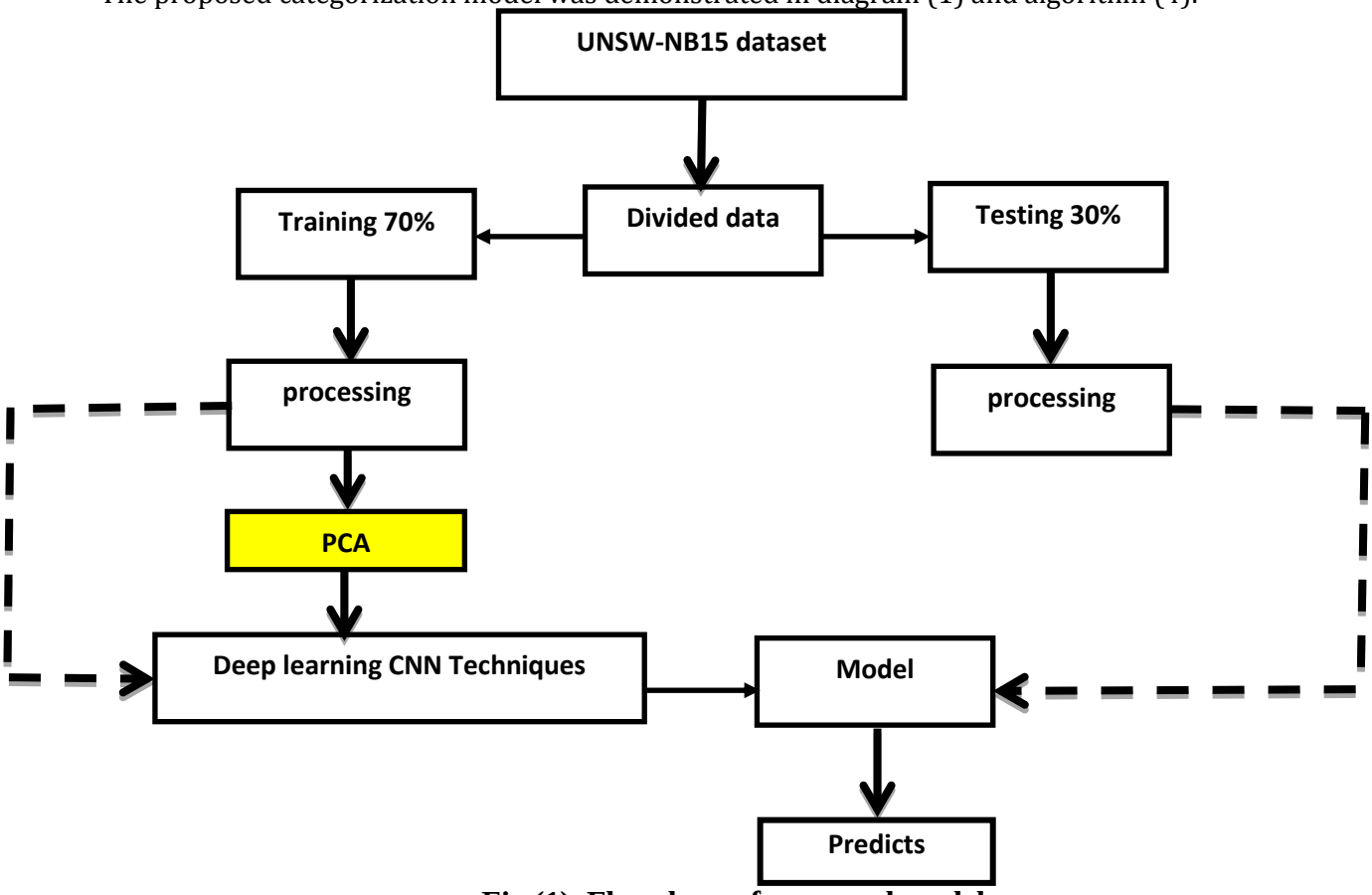


Fig.(1). Flowchart of proposed model

Algorithm 4

Input: UNSW-NB15 dataset

Output: Accuracy of NIDCNN classification model

- Begin
- Load UNSW-NB15 dataset.
- Call Algorithm 1 to divide dataset .
- Call Algorithm 2 to Standardized dataset .

- Call Algorithm 3to calculate Reduce features using PCA
- Build classification NIDCNN model consist of these layers:

- Nine-layer convolutional neural network
- Maximum pooling is six layers
- 8 layers of leaky ReLU
- 1 flat layer; 3 dense layers

- Return (accuracy)
- End

5. Experimental Results and Discussions

With the UNSW-NB15dataset, the new standard intrusion detection data set, deep learning CNN methods using PCA are tested. These algorithms are tested on an Intel(R) Core(TM) i7-8565U CPU running at 1.80 GHz or 1.99 GHz, 10 GB of Memory, a 64-bit operating system, and Python 3.6.

all the data textual converted to numerical form. data is divided into testing and training data. The proposed are built using PCA the most often used linear feature extraction techniques. Precision, recall, accuracy, and F-score, According to the pre-processing methodology utilized the results of the proposed system are split into two sections: first without the use of any feature reduction techniques, and second using PCA to reduce features in three scenarios (PCA-10, PCA-15, PCA-20), factors mentions up are used to compare the models' performances

5.1 performance evaluation

For the purpose of evaluating the suggested NIDCNN approach, we used a variety of evaluation techniques., measures are used to assess a classifier's accuracy, F-Score, precision, and sensitivity (Recall)[31,32].

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad (7)$$

$$F_1 = 2 * \frac{precision*recall}{precision+recall} \quad (8)$$

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

Where, correspondingly, the acronyms for positive and true negative are TP and TN, whereas false positive and false negative are denoted by FP and FN, respectively[31,32].

5. 2 results and discussions

The NIDCNN model was developed specifically to handle input that is only one dimension. Researchers have previously employed a number of general strategies as well as supplementary deep learning-based techniques for the identification of network breaches. For practice take 70% and traineeship take 30%, these dataset partitions of the total data. We measured the accuracy, precision, recall, and F-score

of the NIDCNN model to assess its effectiveness. Each measure is explained separately in Equations (7 to 10) .

using the proposed model with 42 features without feature reduction techniques (pure), the outcomes were a time of 0.532 seconds, 100% accuracy, 100% precision, 31% recall, and a 48% F-score.
table (1) displays these results and the chart explained figure (2).

Table 1- Pure proposed model

Pure model	Performance 100%
Accuracy	**100**
Precision	**100**
Recall	**31**
F-score	**48**

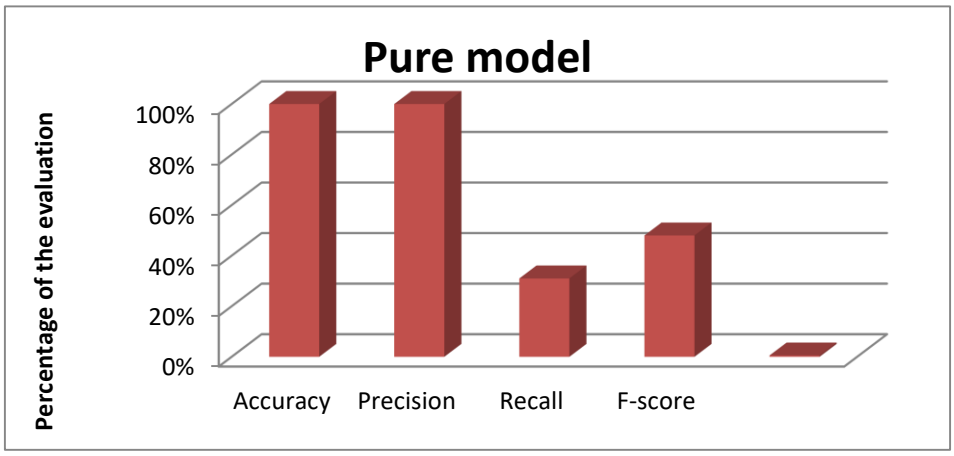


Fig.(2) pure model

the PCA Features Reduction Technique are shown three methods, first is when applying PCA-10,(take 10 features), table (2) get the evaluation results, and figure (3) explains the PCA Technique.

Table (2). PCA-10 features reduction.

PCA-10 Method	Performance 100%
Accuracy	**100**

Precision	**100**
Recall	**63**
F-score	**79**

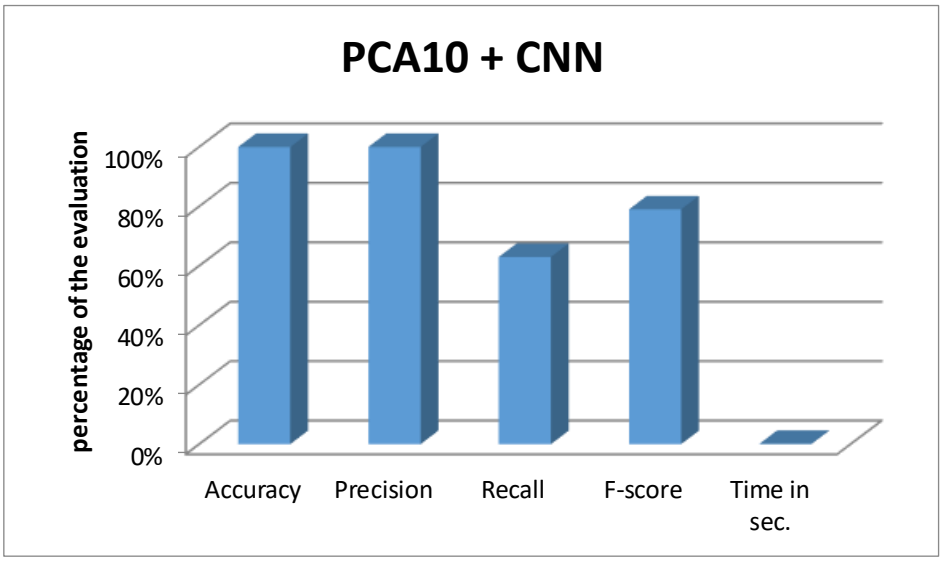


Fig.(3) PCA-10 feature reduction

the second is when applying PCA-15, table (3) get the evaluation results, and figure (4) explains the PCA Technique.

Table (3). classification model with PCA-15 features reduction.

Accuracy	**100**
Precision	**100**
Recall	**63**
F-score	**79**

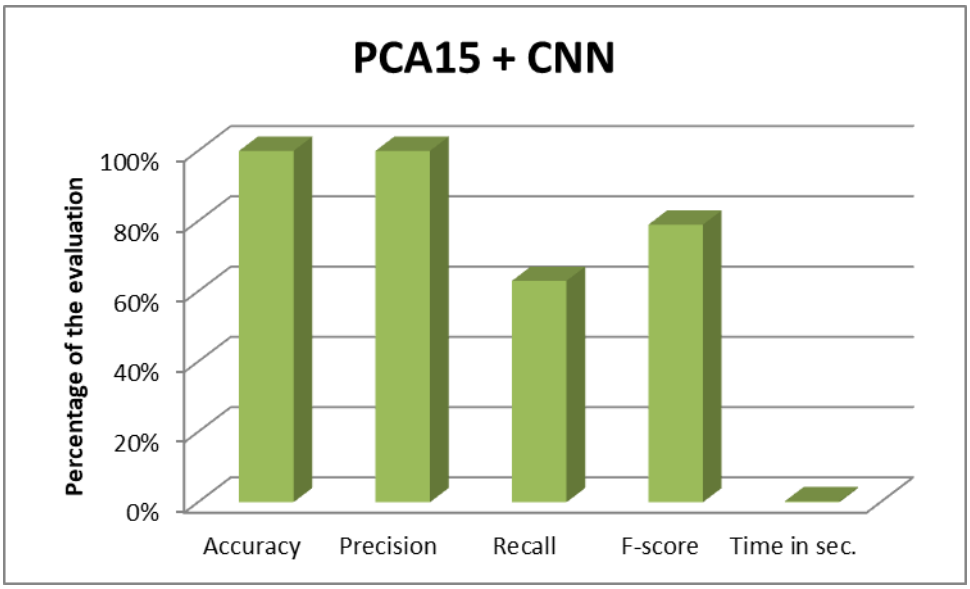


Fig.(4) PCA-15 feature reduction

the third is when applying PCA-20, table (4) get the evaluation results, and figure (5) explains the PCA Technique.

Table (4). classification model with PCA-20 features reduction.

PCA-20 Method	Performance 100%
Accuracy	100
Precision	100
Recall	63
F-score	79
Time in sec	0.33

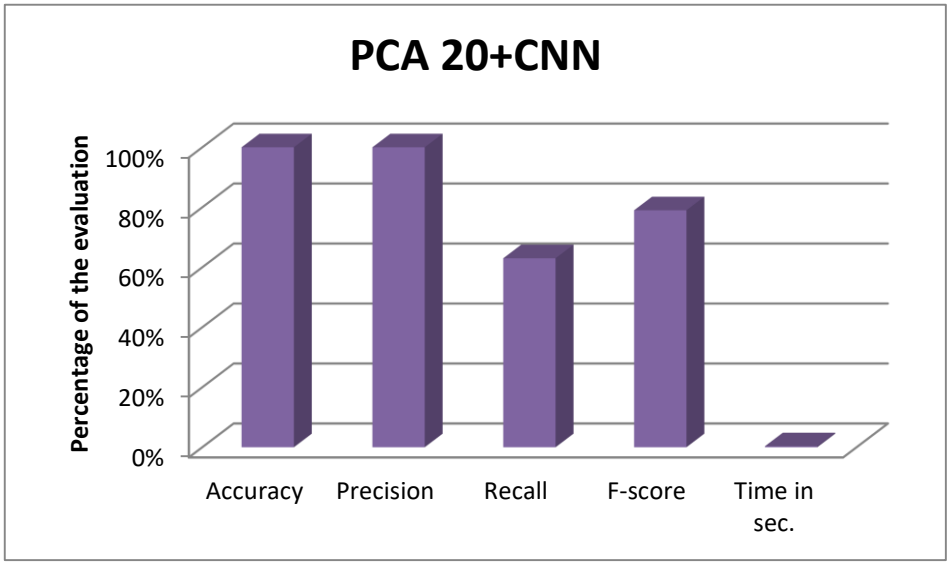


Fig.(5) proposed model with PCA-20 feature reduction

Table (1) to (4) shows that employing the suggested 1D-CNN with PCA-10 based approaches in time 0.106, we obtained 100% testing accuracy, 100% precision, 63% recall, and a 79% F-score. The results are remarkably equivalent when utilizing 1D-CNN with PCA-15 based techniques in time of 0.29 to achieve testing accuracy, precision, recall, and F-score of 79%, 100%, and 100% respectively. The results of the measurements, we obtained 100% testing accuracy, 100% precision, 63% recall, and a 79% F-score with PCA-20 in time 0.313 in sec. however, were 100% accuracy, 100% precision, 31% recall, and 48% F-score, in time 0.532, when using a model without feature reduction techniques. Table (5) shows what was explained in the previous tables, and figure (6).

Table(5).Suggest model with and without reduction techniques

Method	Accuracy 100%	Precision 100%	Recall 100%	F-score 100%	time in sec 100%
Deep Learning (CNN) pure	100%	100%	31%	48%	0.532
PCA10 + CNN	100%	100%	63%	79%	0.106
PCA15 + CNN	100%	100%	63%	79%	0.29
PCA 20+CNN	100%	100%	63%	79%	0.33

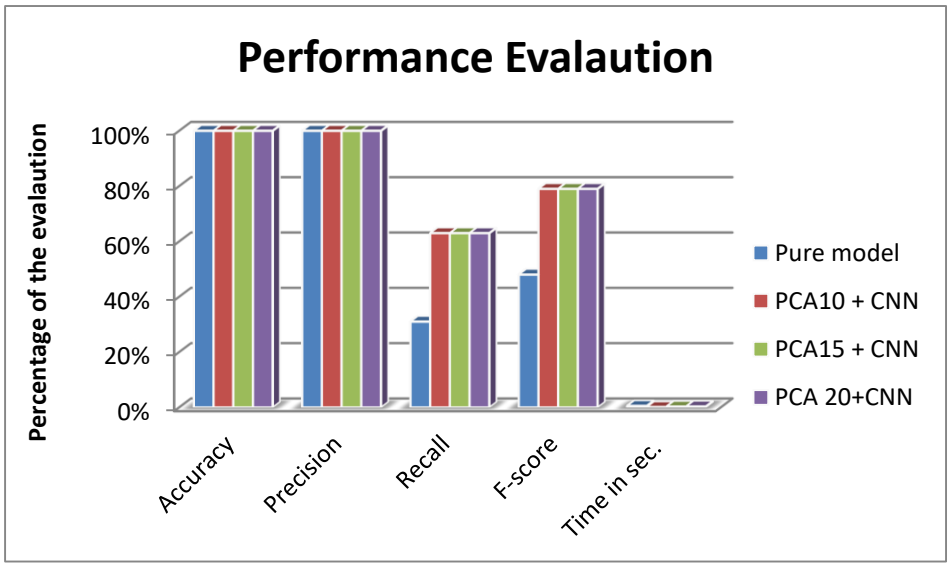


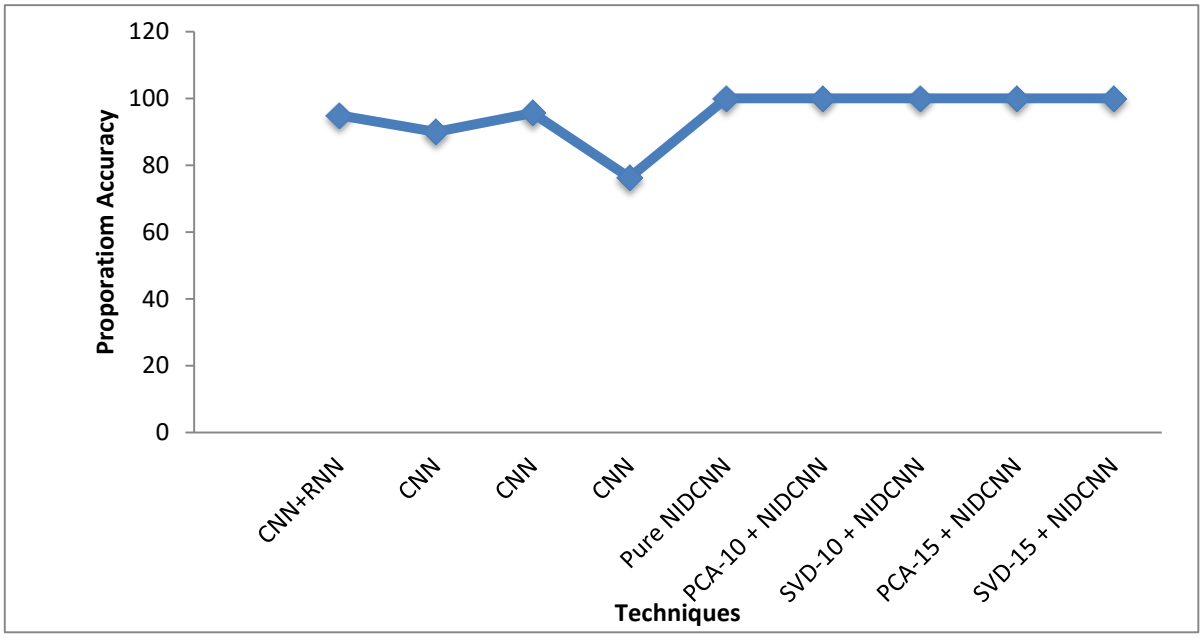
Fig.(6) Explained the previous tables.

5.3 Comparative Findings from Relevant Studies

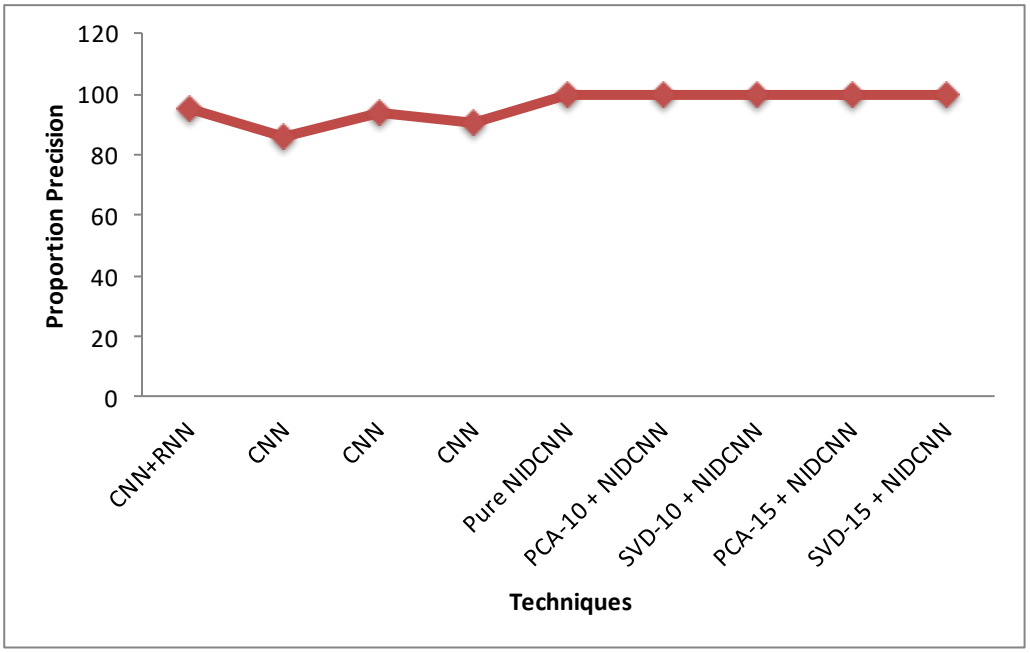
A thorough comparison of the architecture used with the UNSW-NB15 dataset can be seen in Table (7) figures (7,8,9, and 10) show the type of technique and performance evaluation to the same data.

Table (7)

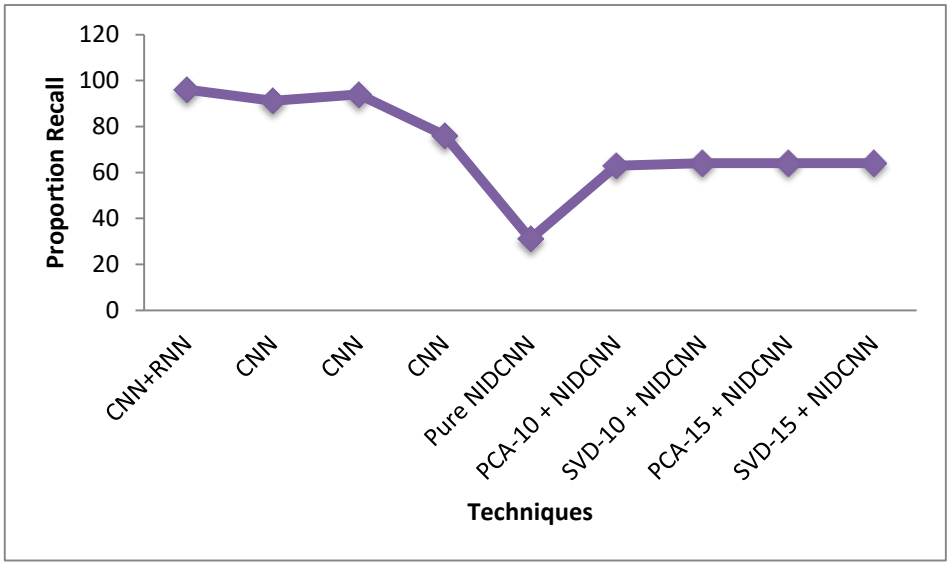
	Ref. No.	Technique	Accuracy%	Precision %	Recall %	F-score %
	[8]	CNN+RNN	94.98	95	96	98.5
	[9]	CNN	89.93	86.15	91.15	90.43
	[10]	CNN	95.6	94	94	94
	[11]	CNN	76.3	90.4	76.1	78.2
Our Methods		**Pure NIDCNN**	**100**	**100**	**31**	**48**
		PCA-10 + NIDCNN	**100**	**100**	**63**	**78**
		SVD-10 + NIDCNN	**100**	**100**	**64**	**78**
		PCA-15 + NIDCNN	**100**	**100**	**64**	**78**
		SVD-15 + NIDCNN	**100**	**100**	**64**	**78**



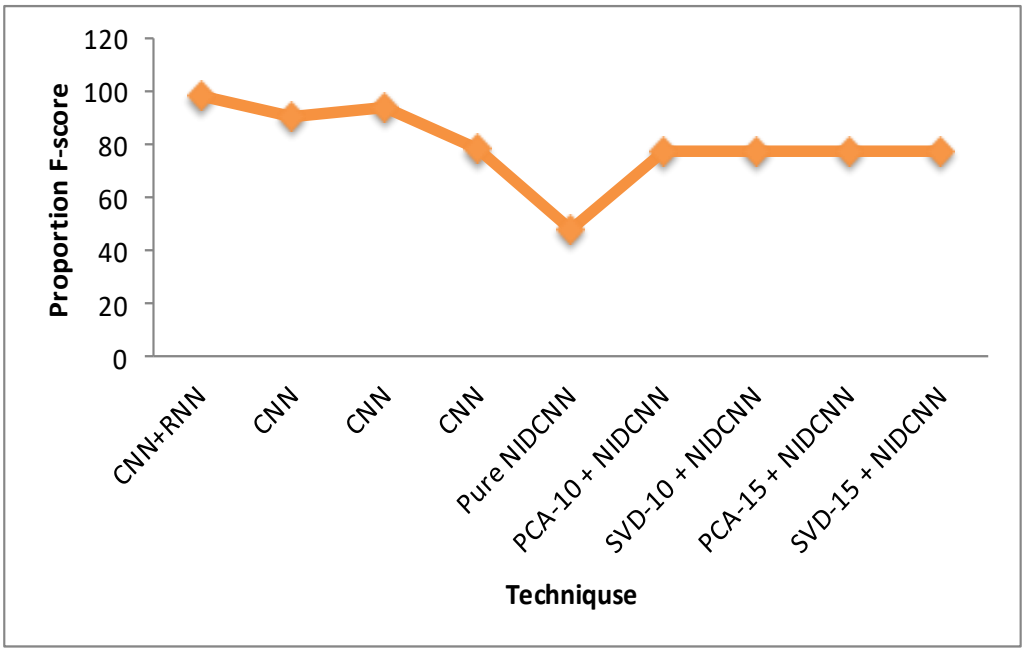
Fig(7).Relation between Accuracy and Techniques



Fig(8).Relation between Precision and Techniques



Fig(9).Relation between Recall and Techniques



Fig(10). Relation between F-Score and Techniques

6. Conclusions

proposition a 1D-CNN-based proposed NIDCNN model for identifying both normal and abnormal network packets. In order to execute multi-class classification detection, we applied the most recent algorithms deep learning and 1D-CNN. The proposed model design is simple uses little processing power. We achieved a total accuracy of 100% with this approach. Additionally, PCA is the method that

reduces dimensionality most commonly. In essence, it shrinks a big data set's high dimensions to lesser dimensions, which speeds up storing and processing of the data makes it easier to understand. It is a statistical method that retains the most information while removing extraneous noise and data. Hence, results with (DR) are substantially better than without it. The work can be expanded to include the crucial aspects of intrusion detection,using PCA techniques led to reducing in the size of data and a limited number of dimensions so take time lesser than without using PCA made data improved increasing accuracy and effective operation algorithms and the classification model becomes simpler all these results gives more idea to using other reduce dimensions method to reach the best level to take the better features., Simulation results have shown that using PCA gives better results.

7-The Future Scope

1-With the help of the proposed NIDCNN model, network intrusion can be detected in real-time, giving rise to the possibility to stop any potential intrusion problems and guaranteeing the security of user data.

2-is compatible with a variety of IDS types, including host-based and application-based IDS.

3-Try using Linear Discriminant Analysis (LDA) or other feature reduction methods while processing the dataset.

4-utilizing an intrusion data-containing dataset that is distinct from the ones used in this study., as KDD99 benchmark data collection. that the UNSW-NB15 data set is more complicated than the KDD99 data set.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Ahmed A. Al-fetouh Saleh: background work, conceptualization, methodology, Inbithaq A. Shakir: Dataset collection, implementation, result analysis and comparison, preparing draft. Hazem M. El-Bakry: editing draft, visualization.

References

[1] John Goodall et al.," The Work of Intrusion Detection: Rethinking the Role of Security Analysts" *Proceedings of the Tenth Americas Conference on Information Systems*, New York, August 2004.
[2]P. Garcı´a-Teodoro et al.," Anomaly-based network intrusion detection: Techniques, systems and challenges" *computers & security* 28 (2009) 18–28.
[3] Salima Omar et al.," Machine Learning Techniques for Anomaly Detection: An Overview" *International Journal of Computer Applications* (0975 – 8887), October 2013.
[4] M. Ferrag et al., "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, 2020.
[5]Mohammad Sazzadul Hoque et al.," an implementation of intrusion detection system using genetic algorithm" *international journal of network security & its applications* (ijnsa), march 2012.
[6] M. e. al., "Deep Learning for Cyber Security Intrusion Detection :Approaches ,Datasets , and Comparative Study," *Journal of Information Security and Applications,* 2020.
[7] a. N. M. Hazem M.EL-Bakry, "Areal time intursion detection algorithm for network security," WSEAS *Transactions on communications* , pp. 1222-1234, december 2008.
[8] R. Almarshdi et al. "Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network "pages1197–1210,2021.
[9] M. Hassan et al. ,"A hybrid deep learning model for efficient intrusion detection in big data environment", 386-396, March 2020.

[10] P. Wu and H. Guo, "LuNet: A Deep Neural Network for Network Intrusion Detection," [cs.AI] 6 Oct 2019.
[11] M. Azizjon et al., "1D CNN Based Network Intrusion Detection with Normalization on Imbalanced Data," *International Conference on Artificial Intelligence in Information and Communication* (ICAIIC), Fukuoka, Japan, 19-21 February 2020.
[12]A. Alsaheel et al., "ATLAS: A Sequence-Based Learning Approach or Attack Investigation," *Proceedings of the 30th USENIX Security Symposium*, pp. 3005–3022, August 2021.
[13] L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," *Complex Adaptive Systems Conference Theme: Big Data, IoT, and AI for a Smarter Future Malvern, Pennsylvania*, June 16-18, 2021.
[14] M. Hooshmand and D. Hosahalli, "Network Anomaly Detection Using Deep Learning Techniques," CAAI *Transactions on Intelligence Technology*, 228–243, 2022.
[15] F. Sultana et al., "Advancements in Image Classification Using Convolutional Neural Network," in Proceedings of the 2018 4th International Conference on Research in Computational Intelligence and *Communication Networks* (ICRCICN), p122–129,Kolkata, India, November 2018.
[16] A. Oprea, "The Use of Principal Component Analysis (PCA) in Building Yield Curve Scenarios and Identifying Relative-Value Trading Opportunities on the Romanian Government Bond Market," *Journal of Risk and Financial Managemen*t. 247, 2022.
[17] Lin, Y., et al., " The individual identification method of wireless device based on dimensionality reduction and machine learning", *The Journal of Supercomputing*, 3010-3027,2017.
[18] Verleysen M., François D,"The Curse of Dimensionality in Data Mining and Time ",*Computational Intelligence and Bioinspired Systems*. , 2005.
[19] Zebari , R., etal.,." A Comprehensive Review of Dimensionality Reduction Techniques for Feature Selection and Feature Extraction". *Journal of Applied Science and Technology Trends*, 56 – 70,2020.
[20] Mahmood, M. R. and Abdulazeez, A. M. "Different Model for Hand Gesture Recognition with a Novel Line Feature Extraction",. 52–57,2019, doi: 10.1109/ICOASE.2019.8723731.
[21] Arif, M. T. Book Review, Asia Pacific J. Public Heal., pp. 507–508,2010, doi: 10.1177/1010539510380245.
[22] Ning, C. and You, F. "Data-driven decision making under uncertainty integrating robust optimization with principal component analysis and kernel smoothing methods", *Comput. Chem. Eng*., pp. 190–210, doi: 10.1016/j.compchemeng.2018.
[23] Gajjar, S., Kulahci, M. and Palazoglu, A. "Real-time fault detection and diagnosis using sparse principal component analysis," *J. Process Control*, 112–128, 2018.
[24] M. L. e. al., "Interpolation in Time Series: An Introductive Overview of Existing Methods, Their Performance Criteria and Uncertainty Assessment,", p. 796, 2017.
[25] Pořízka, P., et ,al.,". On the utilization of principal component analysis in laser-induced breakdown spectroscopy data analysis", , pp. 65–82, doi: 10.1016/j.sab.2018..
[26] Liu, J., Wang, et,al., "Advanced Energy Storage Devices Basic Principles", *Analytical Methods, and Rational Materials Design*, 2017.
[27] Fujiwara, T., et,al.,. "Supporting Analysis of Dimensionality Reduction Results with Contrastive Learning",*Comput. Graph*., pp. 45–55,2020.
[28] Jackson, J. E. "A User' s Guide to Principal Components". by J. *Edward Jackson Review* by: Brian D. 1991.
[29] F. Sultana et al., "Advancements in Image Classification Using Convolutional Neural Network," *4th International Conference on Research in Computational Intelligence and Communication Networks* (ICRCICN), pp. 122–129, Kolkata, India, November 2018.
[30]S. Brunton and J. Kutz, "Singular Value Decomposition (SVD)," *Data-Driven Science and Engineering* (pp.3-46), 2019.
[31] Sadiq Hussain et al.," Prediction Model on Student Performance based on Internal Assessment using Deep Learning", iJET – , 2019.
[32] Mathieu Lepot et al.," Interpolation in Time Series: An IntroductiveOverview of Existing Methods, Their Performance Criteria and Uncertainty Assessment", *www.mdpi.com/journal/water*, 2017.