I.J. Wireless and Microwave Technologies, **2023, 4, 35-46**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.04.05

Evaluating Linear and Non-linear Dimensionality Reduction Approaches for Deep Learning-based Network Intrusion Detection Systems

Stephen Kahara Wanjau*
Department of Computer Science, Murang'a University of Technology, Kenya
E-mail: steve.kahara@gmail.com
ORCID iD: https://orcid.org/0000-0002-6567-6912
*Corresponding Author

Geoffrey Mariga Wambugu
Department of Information Technology, Murang'a University of Technology, Kenya
E-mail: gmariga@mut.ac.ke
ORCID iD: https://orcid.org/0000-0002-0250-0135

Aaron Mogeni Oirere
Department of Computer Science, Murang'a University of Technology, Kenya
E-mail: amogeni@mut.ac.ke
ORCID iD: https://orcid.org/0000-0002-3167-9429

Received: 12 October, 2022; Revised: 15 December, 2022; Accepted: 12 March, 2023; Published: 08 August, 2023

Abstract: Dimensionality reduction is an essential ingredient of machine learning modelling that seeks to improve the performance of such models by extracting better quality features from data while removing irrelevant and redundant ones. The technique aids reduce computational load, avoiding data over-fitting, and increasing model interpretability. Recent studies have revealed that dimensionality reduction can benefit from labeled information, through joint approximation of predictors and target variables from a low-rank representation. A multiplicity of linear and non-linear dimensionality reduction techniques are proposed in the literature contingent on the nature of the domain of interest. This paper presents an evaluation of the performance of a hybrid deep learning model using feature extraction techniques while being applied to a benchmark network intrusion detection dataset. We compare the performance of linear and non-linear feature extraction methods namely, the Principal Component Analysis and Isometric Feature Mapping respectively. The Principal Component Analysis is a non-parametric classical method normally used to extract a smaller representative dataset from high-dimensional data and classifies data that is linear in nature while preserving spatial characteristics. In contrast, Isometric Feature Mapping is a representative method in manifold learning that maps high-dimensional information into a lower feature space while endeavouring to maintain the neighborhood for each data point as well as the geodesic distances present among all pairs of data points. These two approaches were applied to the CICIDS 2017 network intrusion detection benchmark dataset to extract features. The extracted features were then utilized in the training of a hybrid deep learning-based intrusion detection model based on convolutional and a bi-direction long short term memory architecture and the model performance results were compared. The empirical results demonstrated the dominance of the Principal Component Analysis as compared to Isometric Feature Mapping in improving the performance of the hybrid deep learning model in classifying network intrusions. The suggested model attained 96.97% and 96.81% in overall accuracy and F1-score, respectively, when the PCA method was used for dimensionality reduction. The hybrid model further achieved a detection rate of 97.91% whereas the false alarm rate was reduced to 0.012 with the discriminative features reduced to 48. Thus the model based on the principal component analysis extracted salient features that improved detection rate and reduced the false alarm rate.

Index Terms: Classification, Dimensionality Reduction, Feature Extraction, Network Intrusion Detection System, Isometric Feature Mapping, Principal Component Analysis.

1. Introduction

A Network Intrusion Detection System (NIDS) is a dynamic system that constantly monitor and analyze network traffic to detect any deviance from the normal activities of passing traffic as intrusions [1]. Research in this area is motivated by the need to improve the efficiency and accuracy of the NIDSs. Recent works involving NIDSs have seen researchers shifting their attention to intrusion detection technology centered on machine learning methods [2, 3]. These methods have been known to reduce false alarm rates and produce more accurate intrusion detection systems. Machine learning algorithms require vast amounts of data to learn and model high level abstractions from input data. However, their performance can degrade with too many input features. Generally, a high number of input features often make a predictive modeling task very challenging, a phenomenon normally referred to as the curse of dimensionality [4] as the model tends to overfit. Thus, it is desirable that the number of input features is significantly reduced to improve the performance of intrusion detection systems using features that are more discriminative and representative [5].

Deep learning is an offshoot of machine learning that encompass consecutive information processing layers that are organized in a hierarchical fashion for pattern classification and high-level features extraction have been the focus of modern day researchers in network intrusion detection[6-8]. Deep networks facilitate design of resilient and adaptive network intrusion detection systems capable of learning and accurately detecting both known and novel or zero-day network behavioural features, subsequently denying intruders systems access and decreasing the risk of compromise [9]. Scholars are turning their attention to the current trend of deep learning as they have a theoretical guarantee to avoid the curse of dimensionality for an important class of problems compared to shallow networks [4].

Successful use of predictive modelling is greatly contingent on unfettered access to adequate volumes of accurate, relevant and clean data. In the modern day organizations, network monitoring devices collect large volumes of traffic data at high rates occasioned by real time streaming. This data is synonymous to big data often described using three attributes namely high volume, high velocity, and contains greater variety [10] and contains too many attributes, some of which are irrelevant and unstructured in nature [11]. Subsequently, there is need for an effective approach that extracts discriminative features from such voluminous high-dimensional network traffic data. Dimensionality reduction, a data pre-processing technique intended to remove redundant features, irrelevant and noisy data, with the purpose of improving the accuracy of learning features and lower the model training time [12] is being applied in the design of deep learning models.

A corpus of dimensionality reduction techniques have been suggested and implemented in the literature utilizing feature selection and extraction methods[1,5,13] .The objective is to isolate a subset of features that is derived from the entire input features dataset for efficient model training. In the network intrusion detection domain, dimensionality reduction techniques for feature extraction have been applied in several works where massive volume of data are involved. The authors in [5] used two feature dimensionality reduction methods namely the Principal Component Analysis and Auto-Encoder, an instance of deep learning, to build various classification models for designing an intrusion detection system. The experimental results showed better performance in terms of Accuracy, Detection Rate, False Alarm Rate, and F-Measure with the low-dimensional features from 81 to 10. The Bayesian Network, Quadratic Discriminant Analysis, Random Forest, and Linear Discriminant Analysis classifiers were trained and tested on the CICIDS2017 dataset for both binary and multi-class classification. The resulting Random Forest model maintained a high accuracy of 99.6% in both classifications.

The study by [1] offered a new hybrid dimensionality reduction technique that combined two approaches namely principal component analysis and information gain using an ensemble of classifiers based on support vector machine, multilayer perceptron and instance-based learning algorithms for intrusion detection. The ensemble method was evaluated based on three well-known datasets, namely NSL-KDD, Kyoto 2006+, and ISCX 2012. Experimental results demonstrated that discrete features considerably outperformed individual approaches to attain high accuracy and low false alarm rates.

The key objective of this research was to illustrate how to lower the number of dimensions in a network intrusion dataset utilizing and present a comparison in the performance of a linear and non-linear feature dimentionality reduction techniques. The study employed both the Principal Component Analysis and Isometric Feature Mapping respectively. Ideally, these techniques pick out a small portion of features from a huge dataset, combine them and work out new features. The resultant new features encompass the most significant data from the original dataset in relation to the situation where the technique is being used. To proof the concept and verify impact of feature dimensionality reduction, the study utilized the CICIDS2017 benchmark dataset technologically advanced by the Canadian Institute for Cybersecurity [14]. This dataset consist of modern-day benign activities and malignant attacks that describes the concurrent network traffic. It presents a comprehensive knowledge of modern day network attacks conducted and conceptual knowledge about the different network devices, protocols and application models [15]. Contained in this dataset is the normal background traffic that was collected by means of B-profile system and constructs the abstract behaviour of 25 network users created using FTP, SSH, email protocols, HTTP, and HTTPS protocol [16] that accurately mimic an actual network environment. The key contributions of this paper are listed as follows:

1) The study accomplished effective features dimensionality reduction in the CICIDS2017 dataset using PCA and ISOMAP algorithms.
2) Improved predictive performance of the hybrid deep learning-based intrusion detection model that combines the CNN+Bi-LSTM model with dimensionality reduction algorithm in an ensemble approach. The prominent discriminating features that are embedded in the CICIDS2017 dataset were identified.

The rest of this paper is structured as follows. Section 2 briefly reviews exisiting literature on the subject domain. Section 3 describes the dimensionality reduction techniques namely the Principal Component Analysis (PCA) and the Isometric Feature Mapping (ISOMAP) used in this study. Section 4 provides a description of the proposed approach including the experimental setup. Section 5 presents the experiment and the results. Finally, Section 6 draw conclusions and provide future research directions.

2. Literature Review

Dimensionality reduction, a process of reducing number of features in a dataset while retaining as much information as possible, is a critical component in machine learning tasks such as regression or classification. The higher the number of features, the more difficult it is to model them, leading a commn problem known as the curse of dimensionality. High dimensional data portends the risk overfitting the machine learning model, difficulty in clustering similar features, and increased space and computational time complexity [17, 18]. Therefore, it is essential to reduce the dimensionality by projecting the data to a lower dimensional subspace that captures the essence of the data.

Various methods have been applied by researchers to reduce dimensionality of features while developing machine learning models for network intrusion detection systems. The study by [20] combined feature selection and machine learning algorithms to model an intrusion detection system and tested using the NSL-KDD dataset where 16 fearures were selected from the 39 features contained in the dataset. Abdulhammed et al [5] used two feature dimensionality reduction approaches namely Auto-Encoder (AE) and Principle Component Analysis (PCA) for dimensionality reduction to model Intrusion Detection Systems using machine learning algorithms. These approaches reduced feature dimensions from 81 to 10 in the CICIDS2017 dataset, while attaining an accuracy score of 99.6% in both multi-class and binary classification. The study by [19] used three different dimensionality deduction techniques namely PCA, Uniform Manifold Approximation and Projection (UMAP) and T-Distributed Stochastic Neighbor Embedding (t-SNE) in designing multiple intrusion detection systems using different machine learning algorithms. The models were tested on three different datasets for binary classification of incoming attacks between benign activity and DDoS Attacks. The 78 features in the initial Friday Afternoon DDoS attack dataset were reduced to 2 features using all the three dimensionality reduction algorithms.

A variety of deep learning models of different depths have been built and analyzed for binary and multiclass classification. A comparative study between PCA and t-SNE for dimensionality reduction while applied in Android Malware Detection system concluded that t-SNE performed better than PCA in terms of preserving data and overall performance [21]. In his work, Niyaz [22] utilized Self-taught Learning (STL), a deep learning-based approach, to classify the different classes present in the NSL KDD benchmark dataset. The study performed an evaluation of attack impact on network services running in the SDN environment and e response time and loss of service delivery in different attack scenarios. The study by [23] implemented deep learning solution for detecting attacks based using Long Short-Term Memory (LSTM). PCA and Mutual information (MI) methods were utilized for dimensionality reduction and feature selection and the solution tested on the KDD99 benchmark data set. The experiment results showed that models based on PCA attain the best training and testing accuracy in both binary and multiclass classification. The work of [24] demonstrated how to lower the number of dimensions utilizing AE over the PCA method where the NSL KDD benchmark dataset was used. The auto-encoder does not make any assumptions about the data's linearity as compared the PCA method that assumes that the findings are linear for the classification outcomes. Alotaibi, et al [25] study used PCA, linear dimensionality reduction algorithm, alongside the decision trees and Deep Neural Network algorithms to build a network intrusion detection model. The model used decision trees to carry out preliminary screening of the pre-processed data to be detected before engaging PCA as an input to perform a secondary decision using the deep neural network. The resultant DT-PCA-DNN model was tested on NSL-KDD dataset where after one-hot encoding, the dataset had a data dimension of 122. The PCA method was observed to lower the dimension of the data consequently achieving higher detection accuracy and faster detection rate that effectively solves the real-time intrusion detection problem.

3. Dimensionality Reduction Approaches

The research presented in this paper examines both linear and non-linear dimensionality reduction techniques for the purpose of decreasing the computational processing overhead and reducing noise in modeling network intrusion detection systems. These methods endeavour to learn appropriate and simplified data representation from the original dataset with the intention to gain more insight from huge dataset [17]. New features are generated in such a manner that they preserve substantial information as much as possible from the original feature set. Dimensionality reduction, the research work is expected to generate fewer features that would reduce the model complexity, reduce storage space as a

result of fewer data, the fewer features require less computation time. Further, the model accurace improves owing to fewer misleading data.

Dimensionality reduction is usually a pre-processing step for feature extraction and classification tasks and does not automatically reduce the existing features. The method, first and foremost, summarize all features in a dataset into several components according to the chosen algorithm. Considering a set of N-dimensional samples $\bar{x} = \{x_1, x_2, \dots, x_N\}$, where N represents the number of features being monitored. According to [18], the feature extraction process transforms an element $\bar{x} \in \mathbb{R}^N$, which is described by the features $\{x_1, x_2, \dots, x_N\}$, in an element $\tilde{x} \in \mathbb{R}^q$, described by the features $\{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_q\}$, in the case where each new feature $\tilde{x}_j$ is obtained from a mixture of a number of features of $\bar{x}$.

In the literature, feature extraction algorithms can be grouped into two main categories namely linear and non-linear. Fig. 1 illustrates the classification of various dimensionality reduction approaches.

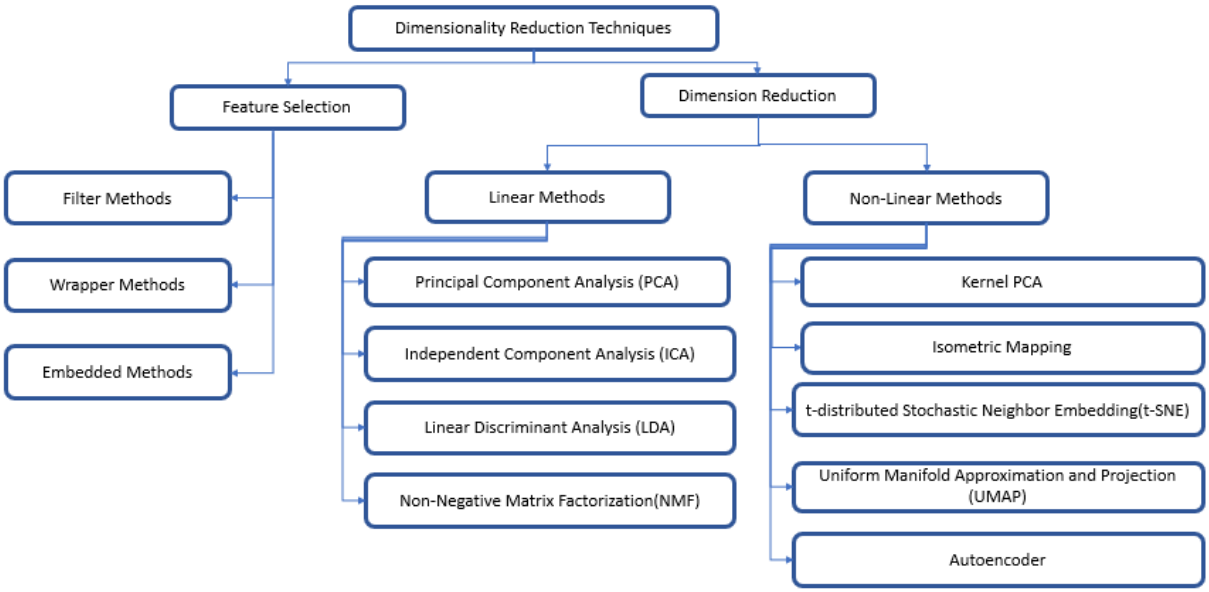

Fig. 1. Dimensionality reduction approaches (Source: *[19]*)

Linear methods tend to be easy to compute than non-linear ones and can be parsed [20]. As such, linear methods are mostly used for early data dimensionality reduction. Nonetheless, given that problems encountered by researchers are also non-linear and time-varying systems in nature, the study also focused on analyzing non-linear feature reduction methods. In this work, we focused on one technique from each of the two categories. These techniques are described in the following subsections.

3.1 Principal Component Analysis

The Principal Component Analysis (PCA) has turn out to be a popular dimensionality reduction technique to project data onto new axes that are orthogonal to each other [21]. The technique is mostly used owing to its inordinate effectiveness and ease of implementation. PCA is moderately computationally cost efficient, capable of dealing with massive datasets, and is extensively utilized as a linear dimensionality reduction technique [22]. As an unsupervised method, PCA performs linear transformations to data comprising numerous variables that are correlated with each other to a lower dimension while preserving the necessary variance present in the data [23]. By reducing the dimension of the initial variables, many highly correlated variables can be transformed into independent or unrelated variables. The PCA technique maps the respective instance of a specified dataset existing in a d dimensional space to a k dimensional subspace in a manner that $k < d$. The new set of k dimensions produced are referred to as eigenvectors or the Principal Components [5], which can be exemplified using the following equation;

$$PC_i = b_1 X_1 + b_2 X_2 + \dots + b_n X_n \tag{1}$$

Where i is the principal component, X_j represents the original feature j, and b_j represents the numerical coefficient for X_j.

A covariance matrix is produced that articulates the correlation existing between the different variables in a dataset. In Mathematical terms, a covariance matrix can be described as a t x t matrix, where t epitomizes the dimensions of the dataset. Every entry in the matrix characterizes the covariance of the corresponding variables. In this study, a 2-Dimensional matrix was considered as input to the 2-Dimensional convolutional neural network used. In the work of

[24], PCA technique was used to identify the best possible number of Principal Components that are necessary for the intrusion detection task. Experiments were conducted on the KDD CUP and UNB ISCX benchmark datasets. Experiment results revealed that the first 10 Principal Components were the most effective for the classification task achieving a classification accuracy of 99.7% and 98.8%, which was approximately similar to the accuracy achieved while using the original 28 features for UNB ISCX and 41 features for KDD CUP, respectively.

3.2 Isometric Feature Mapping

The Isometric Feature Mapping (ISOMAP), a manifold learning algorithm, is a non-linear learning method, that has proved to be an effective dimension reduction tool [25]. Compared to other non-linear dimension reduction approaches, this technique give emphasis to modest algorithmic implementation and circumvents non-linear optimization formulations which are predisposed to local minima. ISOMAP uses the geodesic distance thus finding any curves or convex regions in the underlying manifold measured as if the surface were flat. The geodesic distances amongst any two points in a given image are approximated by graph distance occurring between the two points. The algorithm exploits the shortest-path to estimate the geodesic distance, effectively expressing the data of the high-dimensional space in the low-dimensional space thus minimizing the information lost after the dimension reduction [26].

ISOMAP generates a similarity matrix for eigenvalue decomposition where a global similarity matrix is created using the local information. Consider an original dataset:

$$X = \{x_i\}_1^N, x_i = \left(x_{i1}, x_{i2}, ..., x_{iD}\right)^T \tag{2}$$

Neighborhood parameter k, a target dimension d; the neighborhood of sample points is given as $NE_i\ i = 1, 2, \dots, N$. The output can be expressed as follows:

$$Y = \{y_i\}_1^N, y_1 = \left(y_{i1}, y_{i2}, ..., y_{iD}\right)^T \tag{3}$$

The specific steps followed by the ISOMAP algorithm are as listed below:

1. Generate a neighborhood graph G and proximity matrix from a dataset.
   The Euclidean distance matrix between sample points D_R is calculated first. The distance between any two points is expressed as $D_R(x_i, x_j)$. The following two approaches may be used to create a neighborhood graph.
   a) K-NN: where the matrix D_R, $NE_i\ i = 1, 2 \dots N$ is used to determine the k-nearest neighbors of each sample point.
   b) $\varepsilon - ball$: where we compute the neighborhood set of samples by setting a fixed threshold $\varepsilon\ NE_i = \{x_j | j \neq i, d_r(x_i, x_j) \leq \varepsilon\}\ i = 1, 2, \dots, N$.
   Amid the two approaches, the edge of the neighborhood graph is set to $d_r(x_i, x_j)$ or ∞, in the circumstances where two points are each other neighbors.
2. Compute the geodesic distance (shortest path) matrix DG.
   At this point, the Dijkstra's algorithm is applied with the nearest neighbor graph *G* (constructed by either of the two methods) to find the shortest path distances amongst any two points in the neighborhood graph ($d_G(x_i, x_j)$. Therefore, we can obtain a matrix $D_G = \{d_G(x_i, x_j)\}$ that comprises of the shortest path of all pairs of points in graph G.
   Given the input, a pairwise distance $d(x_i, x_j)$ of data points in the input space, embedding dimension $k \geq 1$ using any of the method would output a k-dimensional representation of the data $Y \in \mathbb{R}^{nxk}$.
3. Constructing d-dimensional Euclidean space embedding that preserves the feature geometry embedded in the space Y.

$$\tau(D_G) = -\frac{Bx(D_G)^2 xB}{2} \tag{4}$$

Where B is the unit matrix and is in the same order with D_G. Eigen decomposition on $\tau(D_G)$ is performed by taking the largest first d eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_d$ and the corresponding Eigen vectors; $V_1, V_2, \dots, V_d$.

ISOMAP was applied in a research work by [27], where an intrusion detection algorithm founded on adaptive ISOMAP was recommended. The NSL-KDD intrusion detection dataset that have 41 are feature attributes was used to conduct experiments. The objective was to assess the impact of the improved ISOMAP algorithm in extracting features on the intrusion detection data using the Support Vector Machine (SVM) classifier. Results from experiments conducted confirmed that with the improved features extraction method, significant improvements in the detection accuracy of R2L, Probe, and U2R attacks were attained. It was demonstrated that the SVM classifier achieved the highest detection rate when the Eigen dimension was set at 16.

4. The Proposed Approach

This section describes in detail the proposed approach including the experimental setup. Essentially, the main objective of this work was to examine the effect of dimensionality reduction on a hybrid deep learning-based network intrusion detection model. The study investigated the impact of both linear and non-linear approaches on the predictive performance of the suggested intrusion detection model.

4.1 Research Design

Experimental research design was adopted for the study which comprises of four stages include data preprocessing, feature extraction and model training, classification, and model evaluation as shown in Fig.3. Experiments were conducted on the CICIDS2017 network intrusion detection dataset to demonstrate how the proposed approach can achieve improved accuracy and practicability. This dataset is publicly available, resembles the true real-world network traffic data and have been used extensively by researchers in network intrusion detection. It is large enough to allow the deep learning algorithms to acquire knowledge more adequate to avoid over-fitting or under-fitting. Collected for a period of five days in a complete network configuration consisting of a network topology that includes switches, modem, routers, firewall and a multiplicity of operating systems for instance Windows, Mac OS X and Ubuntu the dataset is made up of the modern-day benign activities and malignant attacks that describes the contemporary network traffic.

4.2 The Hybrid Deep Learning Model

A hybrid deep learning based model architecture was used that combines a convolution neural network (CNN) with variable kernel dimensions alongside a bi-directional long short-term memory (Bi-LSTM) network to learn and capture the spatial and temporal feature representations from the dataset. The model architecture consists of initial convolution layers that receive feature maps as input. The output of the convolution operation is then pooled to a smaller dimension, then fed into Bi-LSTM layers. This mechanism consists of extracting the inherent characteristics of the flow data by the CNN model and extracting the temporal dependencies by Bi-LSTM layer. Fig. 2 illustrates the architecture of the hybrid deep learning-based model.

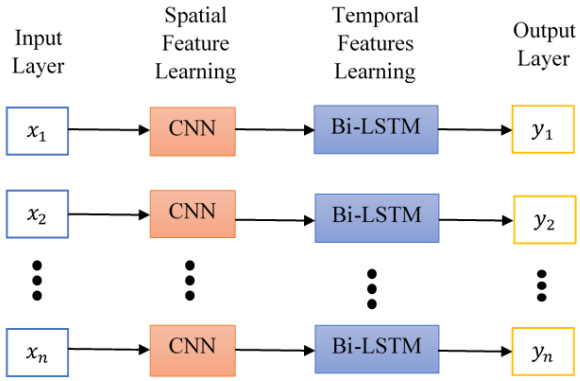

Fig. 2. Architecture of the CNN+Bi-LSTM Model

The design of CNN is based on spatial coherence, and are frequently being used for spatial feature learning. The CNN automatically learns the features of the network traffic data through multi-layer non-linear transformations. After the spatial features are learnt by the CNN, they turn into an input for the Bi-LSTM, which consequently preserves information on temporal dependencies. The Bi-LSTM exploits the techniques of recurrent neural network to learn from temporal data. The workflow process involving various the stages is depicted in Fig. 3.

The framework is comprised of four steps: The first step, data preprocessing is executed on the input raw traffic data with the network traffic features being extracted. Afterwards, the data flow features are passed on to the deep hierarchical network where spatial and temporal features are learnt by the network during training. The output layer received the fusion features that are classified with predictions made on the network flow. Finally, the model is evaluated using a validation dataset.

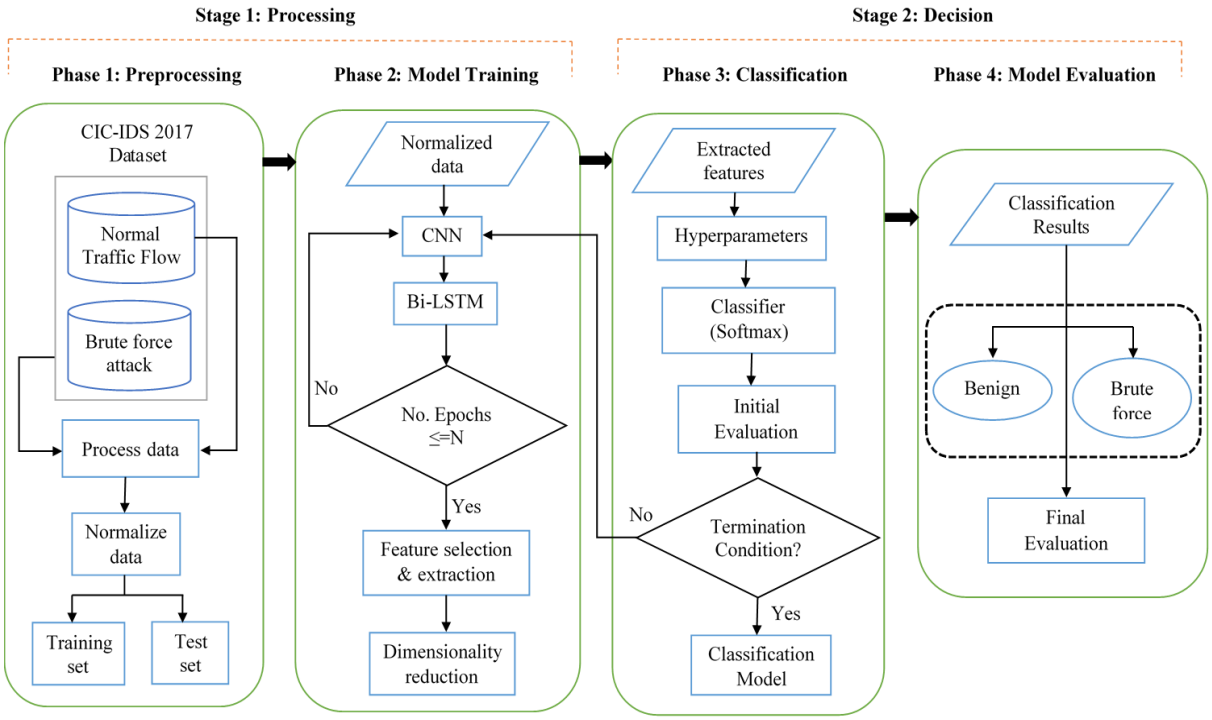

Fig. 3. Framework of the CNN+Bi-LSTM Model for Binary Classification

4.3 Description of Dataset

The CICIDS2017 network intrusion detection dataset that is publicly available was used in this study. The dataset was generated by conceptualizing the behaviour of 25 network users across a range of protocols and has more than 80 network flow features. These features comprises both normal (benign) and seven common attack network flows that bear a resemblance to real world benchmarks. The study utilized the network traffic data captured on a Tuesday that comprises the normal traffic data, SSH-Patator and FTP-Patator attacks as presented in Table 1.

Table 1. FTP-Patator and SSH-Patator attacks in CIC-IDS 2017 Dataset

Day of Week	Network Attack type	Network Attack flows	Benign flows
Tuesday	SSH patator	2511	339,621
	FTP patator	3907	

Each network packet exemplifies a data point in the input sequence. Given that the maximum Ethernet frame size is about 1514 bytes, we considered 1514 as the dimension for each network packet. Therefore, the input is presumed to be a sequence of 1514-dimensional points. The study generated an n x 1514 matrix, in which n represents the number of packets. The PCA and ISOMAP algorithms were used to get the number of features down to 48. This reduced feature vector comprises the feature-set that was provided as input to the input layer of the hybrid deep learning-based model.

4.4 Experiment Setup

All experiments were done on an Intel Core i5 2.50 GHz CPU and 16 GB of RAM. The main hypothesis of the study was that using hybrid deep learning-based IDS, we can decrease time and complexity while retaining better accuracy by representing decreased feature dimensions.

The Python toolbox that includes Jupyter Notebook environment and Keras [28] as a wrapper on top of Tensor-Flow [29] was used as the deep learning framework. To ensure exponential increase in the agility to process data in the TensorFlow, a high performance computer running on GPU-enabled version of TensorFlow was used. A sequence of experiments were conducted to establish the proposed model's efficacy to detect malicious brute force network attacks. The PCA and the ISOMAP classes from Scikit-Learn were used to implement the dimensionality reduction. The CNN+Bi-LSTM intrusion detection model consists of twelve layers. Several trials were done to decide on the hyper-parameters that may produce the greatest performance results. Consequently, the hyper-parameters apportioned to the layers of CNN and Bi-LSTM is described in Table 2. The binary_crossentropy loss function as well as the Adam optimization function were applied to the model. The final model comprises of three convolutional layers, three max-pooling layers, two Bi-LSTM layers, a flatten layer, and three dense layers.

Table 2. A description of the CNN+Bi-LSTM Model

Model Layer	Output Neuron	Kernel Size	Activation Function
Convolution - I	1514 X 4	32	Rectified Linear Unit
MaxPooling - I	757 X 4	-	-
Convolution - II	256 X 6	24	Rectified Linear Unit
MaxPooling - II	128 X 6	-	-
Convolution - III	64 X 3	12	Rectified Linear Unit
MaxPooling - III	64 X 3	-	-
Bi-LSTM	64 X 8	dropout = 0.25	Rectified Linear Unit
Bi-LSTM	64 X 16	dropout = 0.25	Rectified Linear Unit
Flatten	1024	-	-
Dense - I	256	-	Rectified Linear Unit
Dense - II	48	-	Rectified Linear Unit
Dense - III	2	-	Softmax

The building of experiment data sets is as presented in Table 3.

Table 3. Dataset components used in the experiments

Number		Dataset		
		Normal	Attack	Attack Type
Experiment 1	Training	5,500	1,511	SSH patator
	Testing	2,500	1,000	
Experiment 2	Training	7,000	3,000	FTP patator
	Testing	2,500	907	

4.5 Performance Evaluation Metrics

The performance of the NIDS was evaluated based on outputs form the confusion matrix presented in Table 4.

Table 4. Confusion matrix.

		Predicted Class	
Actual class (Ground truth)		**Brute-force**	**Normal (Benign)**
	Brute-force	True Positives (TP)	False Negatives (FN)
	Normal	False Positives (FP)	True Negatives (TN)

From the confusion matrix, common information retrieval evaluation metrics were calculated to evaluate the model's performance after dimensionality reduction. The following five commonly used metrics for evaluating intrusion detection systems were used: Accuracy (ACC), Detection Rate (DR) also called True Positive Rate (TPR), Precision (P), False alarm rate (FAR) and the F-measure (F1-Score).
Accuracy is the measure of the model's ability to correctly classify the dataset instances as either normal traffic or attack.

The Accuracy measure may be derived using Equation 5:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} * 100\% \tag{5}$$

Detection Rate or True Positive Rate designates the number of attacks that are detected divided by the total number of attack instances contained in the dataset. TPR can be computed as shown in Equation 6:

$$TPR = \frac{TP}{TP + FN} * 100\% \tag{6}$$

False alarm rate is the number of False Positives divided by the total number of False Positives and the True Negatives. FAR can be calculated by Equation 7:

$$FAR = \frac{FP}{FP + TN} * 100\% \tag{7}$$

Precision is a measure for the model's ability to be exact. It denotes the number of positive predictions divided by the total number of positive class predictions. A low value points to large number of False Positives. The precision is estimated using Equation 8:

$$P = \frac{TP}{TP + FP} * 100\% \tag{8}$$

The F-measure (F1-Score) is a measure of the model's accuracy and is computed as the weighted harmonic mean of the Precision and Recall. F-Measure is computed as shown in Equation 9:

$$F1 - Score = \frac{2 * precision * \mathrm{Re}call}{\mathrm{Pr}ecision + \mathrm{Re}call} * 100\% \tag{9}$$

5. Results and Discussion

In this section we describe the experiment results using the proposed approach and tested on the CICIDS2017 dataset. The results of the effect of dimensionality reduction using the PCA and ISOMAP techniques, respectively are presented. The extracted features were projected to be of lower dimension spaces, yielding a number of dimensions that would give reasonably good performance results for our intrusion detection model. Normally, a better performing intrusion detection system ought to have, high accuracy score, lower false positive rate and a higher detection rate. Table 5 presents the results obtained from the experiments.

Table 5. Model performance metrics

	Accuracy	Precision	Recall	F1-Score	Detection Rate	False Alarm Rate	Training time (sec)
Dimensionality reduction method							
Principal Component Analysis	96.97	0.97	0.97	96.81	97.91	0.012	170.6
ISOMAP	94.58	0.95	0.96	95.45	94.46	0.27	219.3

The results show that the model reached 96.97% and 96.81% in overall accuracy and F1-score, respectively, when the PCA method was used for dimensionality reduction. This is a better performance compared with the results obtained when the model used the ISOMAP algorithm. Based on the values achieved in precision and recall, it can be perceived that the model trained using the PCA method showed great performance. The false alarm rate was only 0.012, and the detection rate was 97.91% for the same model.

The results demonstrates that PCA algorithm is capable of preserving significant information in the CICIDS2017 dataset, while efficiently minimizing the features dimensions in the dataset used. The study also analysed the run time of each of the models, concentrating on the training time as an indicator of operational value. Each model was subjected to 8 training rounds having similar initialization parameters. The model trained on PCA technique processed the training samples in about 170.6 seconds whereas the total training time for the model trained on the ISOMAP algorithm was 219.3 seconds. These results demonstrates that PCA technique offers an inherent advantage of faster feature extraction compared to ISOMAP. The results agrees with the results of studies reported in the literature where on the same CICIDS 2017 dataset, the linear technique for dimensionality reduction outperformed non-linear technique *[20]*, *[30, 31]*.

The experiment results in Table 6 shows the detection rate and false positive rate while model was tested on the SSH-Patator attack. The results shows that the model using PCA algorithm achieved the highest DR score of 98.91% and a lower FPR of 0.019% compared to the model using ISOMAP algorithm.

Table 6. Comparisons of DR and FPR on SSH-Patator Attack in Experiment 1

Dimensionality Reduction Approach	Detection Rate (%)	False Positive Rate (%)
Principal Component Analysis	98.91	0.019
ISOMAP	97.34	0.12

In Table 7, the model trained on PCA algorithm recorded the lowest DR score, 97.41% compared to the model trained on ISOMAP algorithm which record a DR score of 98.21% in detecting FTP-Patator attacks. In contrast, the model trained on PCA algorithm achieved a FPR score of 0.041% in detecting FTP-Patator attacks, a better score than the model trained on the ISOMAP algorithm, 0.269%.

Table 7. Comparisons of DR and FPR on FTP-Patator Attack in Experiment 2

Dimensionality Reduction Approach	Detection Rate (%)	False Positive Rate (%)
Principal Component Analysis	97.41	0.041
ISOMAP	98.21	0.269

The study further observed that the features such as Flow Duration, Init_Win_bytes_fwd, Subflow Fwd, ACK Flag Count, Average Packet Size, BytesFlow, Inter arrival time (IAT), SYN Flag Count, Active Mean and Min, Total Len Fwd Pck and PSH Flag Count are the leading discriminating features that are rooted in the CICIDS2017 dataset.

This study investigated the performance of two types of dimensionality reduction methods on hybrid deep learning models used for network intrusion detection. The results showed that dimensionality reduction positively affects the performance of the model with the PCA algorithm performing better. This implies that dimensionality reduction can increase performance of deep learning models when using high dimensional data. Further, it was observed that linear dimensionality reduction methods like PCA provide greater performance boost over nonlinear methods on high dimensional data such as the CICIDS2017 data. The performance of our model was analyzed using 6 types of metrics that provided an explicit presentation of the performance of the model with the PCA technique recording better results while compared with the ISOMAP technique. This study has some limitations. First, the study investigated two dimensionality reduction algorithms namely PCA and ISOMAP. While we have confidence that the algorithms selected are representative of the two types of dimensionality reduction techniques, future studies may explore other algorithms.

6. Conclusion and Future Work

Network Intrusion Detection System are being used to persistently monitor and analyze network traffic to detect any deviance from the normal activities of passing traffic. This network traffic is characerised by high dimensionality where current deep learning based NIDS may not handle them accurately and efficiently. Feature selection and dimensionality reduction techniques are implemented to reduce the complexity and increase the performance of deep learning models. This paper investigated the impact of two dimensionality reduction techniques namely PCA and ISOMAP on a network intrusion detection dataset. Dimensionality reduction methods are used in machine learning tasks to effectively decrease data dimensionality in large datasets for efficient data processing problem. These methods are proposed to improve the performance of the models by removing redundant, noisy and irrelevant features from the data thereby reducing computational cost involved in data analysis, improving the training speed, avoiding over-fitting and increasing model interpretability. The PCA and ISOMAP algorithms were applied together with a hybrid deep learning model for network intrusion detection. The high dimensional data points were mapped onto a lower dimensional feature space for classification of network intrusions.

The experiment results espoused the performance of PCA technique as being better than the ISOMAP technique on the CICIDS2017 dataset. The PCA algorithm makes the data convey the best features with fewer dimensions by transforming the coordinate space. As such, this dimensionality reduction technique retains some important features and remove noise and unimportant features, thereby improving the data processing speed, reduce the computational complexity of machine learning classification models while processing high dimensional data. Therefore, using the PCA technique in the design of an intrusion detection system can reduce the system complexity while realizing a better classification accuracy. The results further exemplifies the importance of feature dimensionality reduction techniques in yielding better results with regard to several performance metrics besides the speed of classification. The study identified an explicit number of dimensions at which the model produced reasonably good results while subjected to both the training and test sets. The features were reduced to 48 from the initial 81 features. From the results obtained, the PCA algorithm displayed superior performance compared to the ISOMAP algorithm. It is evident that researchers and practitioners can use dimensionality reduction to improve model performance for network intrusion detection systems. Future work includes testing the approach on another dataset, comparing the impact dimensionality reduction techniques and feature selection methods have on a similar dataset. The trained model may further be extended to be implemented as a NIDS for both online anomaly-based detection and Software Defined Networks.

References

[1] F. Salo, A. B. Nassif and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," Computer Networks, vol. 148, pp. 164-175, 2019.

[2] L. Zhang, M. Li, X. Wang and Y. Huang, "An Improved Network Intrusion Detection Based on Deep Neural Network," IOP Conference Series: Materials Science and Engineering, vol. 563 , pp. 1-8, May 2019.

[3] K. Trieu and Y. Yang, "Artificial Intelligence - Based Password Brute Force Attacks," in Proceedings of the Thirteenth Midwest Association for Information Systems Conference, Saint Louis, Missouri, May 17-18, 2018.
[4] T. Poggio and Q. Liao, "Theory I: Deep networks and the curse of dimensionality," BULLETIN OF THE POLISH ACADEMY OF SCIENCES TECHNICAL SCIENCES, vol. 66, no. 6, pp. 761-773, 2018.
[5] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour and A. Abuzneid, "Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection," Electronics, vol. 8, no. 322, pp. 1-27, 2019.
[6] A. Hijazi, E.-A. Safadi and J.-M. Flaus, "A Deep Learning Approach for Intrusion Detection System in Industry Network," CEUR-WS, vol. 2343, pp. 55-62, 2020.
[7] B. Lee, S. Amaresh, C. Green and D. Engels, "Comparative Study of Deep Learning Models for Network Intrusion Detection," SMU Data Science Review, vol. 1, no. 1, 2018).
[8] Y. Fu, Y. Du, Z. Cao, Q. Li and W. A. Xiang, "Deep Learning Model for Network Intrusion Detection with Imbalanced Data," Electronics, vol. 11, no. 898, p. 13, 2022.
[9] L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," Procedia Computer Science, vol. 185, pp. 239-247, 2021.
[10] R. Chalapathy and S. Chawla, "DEEP LEARNING FOR ANOMALY DETECTION: A SURVEY," ArXiv Preprints, p. ArXiv:1901.03407v2, 2019.
[11] G. Wang, J. Yang and R. Li, "An Anomaly Detection Framework Based on ICA and Bayesian Classification for IaaS Platforms," KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, vol. 10, no. 8, pp. 3 865-3 883, August 2016.
[12] S. Velliangiri, S. Alagumuthukrishnan, S. Iwin and J. Thankumar, "A Review of Dimensionality Reduction Techniques for Efficient Computation," Procedia Computer Science, vol. 169, pp. 104-111, 2019.
[13] W. C. Y. &. S. W. Zong, "Dimensionality Reduction and Visualization of Network Intrusion Detection Data.," in Lecture Notes in Computer Science, 2019, pp. 441-455.
[14] Canadian Institute for Cybersecurity, "Intrusion Detection Evaluation Dataset (CICIDS2017)," Canadian Institute for Cybersecurity, 2017. [Online]. Available: http://www.unb.ca/cic/datasets/ids-2017.html. [Accessed 19 November 2020].
[15] A. Thakkar and R. Lohiya, "Review of the Advancement in Intrusion Detection Datasets," Procedia Computer Science, vol. 167, pp. 636-645, 2020.
[16] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, pp. 41525-41550, 2019.
[17] B. ChandraSekhar, A. Niranjan and G. VenkataRamiReddy, "Dimensionality Reduction using Deep Learning Techniques," International Journal of Psychosocial Rehabilitation, vol. 24, no. 6, pp. 1137-1143, 2020.
[18] K. -M. Zheng, X. Qian and N. An, "Supervised Non-Linear Dimensionality Reduction Techniques for Classification in Intrusion Detection," in 2010 International Conference on Artificial Intelligence and Computational Intelligence, Sanya, China, 2010.
[19] H. Elkassabi, M. Ashour and F. Zaki, "A PROPOSED MODEL FOR DIMENSIONALITY REDUCTION TO IMPROVE THE CLASSIFICATION CAPABILITY OF INTRUSION PROTECTION SYSTEMS," International Journal of Network Security & Its Application (IJNSA), vol. 12, no. 4, pp. 17-37, July 2020.
[20] T. N. Varunram, M. B. Shivaprasad, K. H. Aishwarya, A. Balraj, S. V. Savish and S. Ullas, "Analysis of Different Dimensionality Reduction Techniques and Machine Learning Algorithms for an Intrusion Detection System," in 2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA), Arad, Romania, 2021.
[21] V. Kouliaridis, N. Potha and G. Kambourakis, "Improving Android Malware Detection Through Dimensionality Reduction Techniques," in Machine Learning for Networking: Third International Conference, MLN 2020, Paris, France, 2020.
[22] Q. Niyaz, "Design and Implementation of a Deep Learning based Intrusion Detection System in Software-Defined Networking Environments," 2017.
[23] F. Laghrissi, S. Douzi and K. Douzi, "Intrusion detection systems using long short-term memory (LSTM)," Journal of Big Data , vol. 8, no. 65, p. 16, 2021.
[24] S. M. Yadav and R. Kalpana, "Effective Dimensionality Reduction Techniques for Network Intrusion Detection System Based on Deep Learning," in Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2020 (Algorithms for Intelligent Systems), 1st ed., I. J. Jacob, S. Shanmugam, S. Piramuthu and P. Falkowski-Gilski, Eds., Springer Nature Singapore Pte Ltd, 2022, pp. 507-516.
[25] S. Alotaibi, K. Yadav, A. Aledaily, L. Alkwai, A. K. Yousef Dafhalla, S. Almansour and V. Lingamuthu, "Deep Neural Network-Based Intrusion Detection System through PCA," Mathematical Problems in Engineering, vol. 2022, p. 9, 2022.
[26] I. de-la-Bandera, D. Palacios, J. Mendoza and R. Barco, "Feature Extraction for Dimensionality Reduction in Cellular Networks Performance Analysis," Sensors(Basel), vol. 20, no. 23, p. 10, 4 Dec 2020.
[27] R. Khandelwal, "A Comprehensive Guide to Dimensionality Reduction," 17 January 2022. [Online]. Available: https://arshren.medium.com/a-comprehensive-guide-to-dimensionality-reduction-851624b7377d. [Accessed 28 June 2022].
[28] D. Mishra and S. Sharma, "Performance Analysis of Dimensionality Reduction Techniques: A Comprehensive Review," Advances in Mechanical Engineering, p. 639–651, 2021.
[29] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," Science, vol. 313, no. 5786, pp. 504-507, 2006.
[30] C. Sorzano, J. Vargas and A. Montano, "A survey of dimensionality reduction techniques," arXiv2014, p. arXiv:1403.2877, 2014.
[31] Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," IEEE Access, vol. 7, pp. 42210-42219, 2019.
[32] K. K. Vasan and B. Surendiran, "Dimensionality reduction using Principal Component Analysis for network intrusion detection," Perspectives in Science, vol. 8, pp. 510-512, 2016.
[33] W. Jia, M. Sun, J. Lian and S. Hou, "Feature dimensionality reduction: a review," Complex & Intelligent Systems, vol. 8, p. 2663–2693, 2022.
[34] X. Liu, P. Ma and G. Li, "Research on Adaptive ISOMAP Algorithm and Application in Intrusion Detection," Journal of Physics: Conference Series, vol. 1607, pp. 1-10, 2020.

[35] F. Chollet, "Keras," GitHub repository, 2015.
[36] TensorFlow, "An end-to-end open source machine learning platform," 30 Oct 2020. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf.
[37] R. Abdulhammed, M. Faezipour, H. Musafer and A. Abuzneid, "Efficient Network Intrusion Detection Using PCA-Based Dimensionality Reduction of Features," in 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 2019.
[38] I. Jolliffe and J. Cadima, "Principal component analysis: a review and recent developments," Phil. Trans. R. Soc. A., vol. 374, 2016.

Authors' Profiles

Stephen Kahara Wanjau received his B.Sc. degree in Information Sciences from Moi University, Kenya, in 2006 and MSc. Degree in Computer Systems from Jomo Kenyatta University of Agriculture and Technology, Kenya, in 2018. Currently, he is pursuing a PhD degree in Computer Science at Murang'a University of Technology, Kenya. He is currently serving as the Director of Performance Contract and ISO at Murang'a University of Technology, Kenya. His research interests include Machine Learning, Network Security, Network Intrusion Detection, and Big Data Analytics.

Dr. Geoffrey Mariga is a Senior Lecturer in Murang'a University of Technology. Previously he was Dean and Head of Information Technology (IT) Department, Lecturer, Assistant Lecturer, Examinations Officer and Programmes Coordinator in various higher education institutions in Kenya. Mariga holds a Doctor of Philosophy degree in Information Technology from Jomo Kenyatta University of Agriculture and Technology (JKUAT), M.Sc. in Information Systems from the University of Nairobi and a B.Sc. Mathematics & Computer Science from JKUAT. He has been involved in the design, development and implementation of Computing Curricula in different Universities and Colleges in Kenya. He Chaired Curriculum development panel at the then Kenya Institute of Education currently Kenya Institute of Curriculum Development. His research interests are Machine Learning, Deep Learning, Natural Language Processing, Data mining and Big Data Analytics..

Dr. Aaron Mogeni Oirere received his B.Sc. degree in Computer Science from Periyar University, Salem,Tamilnadu, India in 2007, the M.Sc. degree in Computer Science from Bharathiar University, Coimbatore, Tamilnadu, India in 2010, and the Ph.D. degree in Computer Science from Dr. Babasaheb Ambedkar Marathwada University, Maharashtra, India in 2016. He currently works at the Department of Computer Science, School of Computing and Information Technology, Murang'a University of Technology. His research interest include Automatic Speech Recognition, Human-Computer Interaction, Information Retrieval, Database Management Systems (DBMS), Data Analytics and Hardware & Networking.

How to cite this paper: Stephen Kahara Wanjau, Geoffrey Mariga Wambugu, Aaron Mogeni Oirere, "Evaluating Linear and Non-linear Dimensionality Reduction Approaches for Deep Learning-based Network Intrusion Detection Systems", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.4, pp. 35-46, 2023. DOI:10.5815/ijwmt.2023.04.05