An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning

by Hanafi Hanafi

Submission date: 03-Sep-2022 07:30AM (UTC+0700)
Submission ID: 1891649246
File name: ICAITI_2022_paper_148.pdf (1.05M)
Word count: 6148
Character count: 33569

An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning

Hanafi

[a] Department of computer science, University of Amikom Yogyakarta, Jl. Ringroad Utara Condoncatur Depok, Sleman, 55283, Indonesia
[b] Second Institution, Address, City, ZIP Code, Country

Corresponding author: hanafi@amikom.ac.id.ac.id

***Abstract*—The intrusion detection system was deactivated. An Intrusion Detection System (IDS) is a hardware or software mechanism that monitors the Internet for malicious attacks. It is capable of scanning an internetwork for potentially dangerous behavior or security threats. IDS is responsible for maintaining network activity in accordance with the Network-Based Intrusion Detection System (NIDS) or Host-Based Intrusion Detection System (HIDS). IDS works by comparing known normal network activity signatures with attack activity signatures. In this research, a dimensional reduction and feature selection mechanism called Stack Denoising Auto Encoder (SDAE) succeeded in increasing the effectiveness of Naive Bayes, KNN, Decision Tree, and SVM. The researchers evaluated the performance using evaluation metrics with a confusion matrix, accuracy, recall, and F1-score. Compared with the results of previous works in the IDS field, our model increased the effectiveness up to more than 2% in NSL-KDD Dataset. Moreover, the use of SDAE also improved traditional machine learning with modern deep learning such as Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN). In the future, it is possible to integrate SDAE with a deep learning model to enhance the effectiveness of IDS detection.**

***Keywords*—IDS detection; SDAE; naive Bayes; decision tree; SVM; auto encoder**

Manuscript received 15 Oct. 2020; revised 29 Jan. 2021; accepted 2 Feb. 2021. Date of publication 17 Feb. 2021.
International Journal on Informatics Visualization is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. INTRODUCTION

The number of internet users has increased significantly over the last decade. Additionally, advancements in technology, particularly in the internet, communication, and networking, have resulted in a massive amount of data being generated from a variety of sources, including industry, e-commerce portals, messengers, social media, and healthcare. This massive amount of data is referred to as big data and has four characteristics: high veracity, high velocity, high variety, and high value. Since the advent of big data, the number of attacks has increased as well. In 2019, the internet had been connected to more than 26 billion devices. Additionally, it contributes to the growth of malicious activity on the internet. Intrusion Detection System (IDS) has evolved into a critical tool for enhancing network and computer system security [1][2].

Numerous experts, researchers, and academicians use conventional machine learning mechanisms to improve IDS, including Neural Networks (NN), Support Vector Machines (SVM), K Nearest Neighbors (KNN), Decision Tree 3 (DS3), Multi-Layer Perceptron (MLP), and Auto Encoder (AE). The involvement of conventional shallow learning frameworks (one feedforward network) is ineffective in resolving the autodetection problem for big data. They consistently fail to detect activity attacks, accurately capture attack information, and resolve noise in massive datasets [3][4]. In response to the aforementioned issue, deep learning models such as a deep Auto Encoder (AE), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM) have become increasingly popular in recent years. The illustration of IDS detection is shown in Fig. 1 [5].

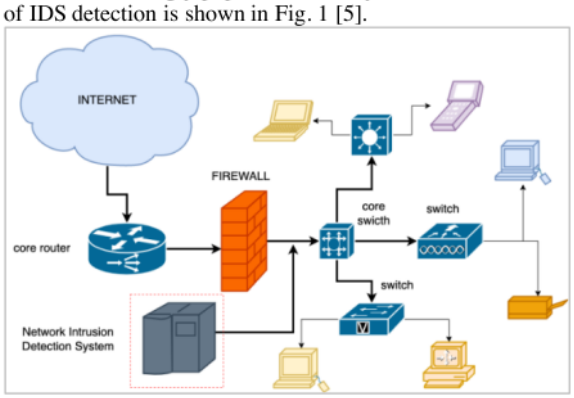

Fig 1. IDS detection illustration

Additionally, the total number of attributes extracted from the internet data that IDS must observe is always enormous, even in small-scale capacity networks. Indeed, the majority of raw data is superfluous and noisy. As a result, the classifier's performance is degraded by the presence of unsuitable features. As a result, it is critical to employ multidimensional reduction frameworks such as the Principal Component Analysis (PCA), Mutual Information (MI), Chi-square, and UMAP [6]. Unlike the previous works, our experiment adopted SDAE to enhance dimensional reduction. The detailed experiment scenario is shown in Fig. 2.

Fig 2. Experiment scenario of IDS detection

In this study, the researchers developed a novel dimensional reduction model based on SDAE, focusing on four aspects including 1) the hybridization between SDAE and KNN, 2) the hybridization between SDAE and Naive Bayes, 3) the hybridization between SDAE and SVM, and 4) the hybridization between SDAE and decision tree. We have applied the proposed model mentioned above to the NSL-KDD dataset.

II. Introduction

A plethora of previous works states that the intrusion detection model has three main methods: deep learning, conventional machine learning, and pattern similarity. In the last few years, deep learning has become the most popular method.

In the beginning, pattern similarity models were mostly used to detect intrusions. Most of them use patterns similar to their main core learning algorithm, and they use attribute similarity to do this [7][8]. Most of the frameworks have already been used for implementation in the past. Knuth Morris Pratt (KMP), Boyer Moore (BM), Boyer Moore Harspool (BMH), Boyer Moore Harspool Sunday (BMHS), Aho-Corasiek (AC), and AC-BM were some of the traditional models that were used to make an Intrusion Detection System. Following the results of the experiments, it was found that an algorithm worked well to speed up the performance of pattern similarity calculations and cut down on the amount of time it took to do them. However, the traditional pattern similarity model has a big problem. They cannot figure out how intrusion detection works. The discovery of a low-cost algorithm that can cut down on the amount of time it takes and the value of false positives has become the main point of this study. When machines become more intelligent, there is still a new study that is worth reading.

Denning [9] was the first to propose IDS machine intelligence, and his study used a multi-algorithm model to detect intrusion detection activity. According to the expert hypothesis, the model created a pattern of several features by hand. First, a modern machine learning model based on SVM was created [10]. The experiment configured KDD99 datasets, resulting in 3 features with an accuracy of 91%, 36 features with an accuracy of 99%, and 41 features with an accuracy of 99%.

A study employing traditional machine learning and KNN succeeded in improving an early model. This model included a K-mean clustering and a KNN classifier [12]. This model evolved into the state-of-the-art IDS intelligence machine for malicious detection known as CANN. Another study proposes the use of a traditional classifier with Random Forest to improve CANN [11]. The hybrid model, which used Random Forest as a core classifier machine, achieved an accuracy of 94.7%. A Random Forest (RF) enhancement using an Artificial Neural Network (ANN) was proposed [12]. When applied to NSL-KDD, the ANN model produced more than 81% of accuracy and 79% classification for malicious detection and network attack classification. A Decision Tree (DT) intrusion detection model based on NSL-KDD was proposed [13]. According to the results of the experiment, DT was successful in achieving effectiveness in the IDS detection classification task. According to the explanation given above, the enhancement of traditional machine learning achieves astounding effectiveness in IDS detection. However, most of them required large-scale pre-processing and complex attribute extraction. When using a machine learning classification method, it is impossible to handle significant intrusion data.

Deep learning, a new type of neural network with a very complex network structure, was introduced in the early decade. Deep learning had achieved tremendous performance in the image processing classification task at the time. Furthermore, deep learning has become the industry standard for dealing with a variety of computer science-related problems such as image processing, voice recognition, and text mining [14][15] [16] [17].

Ref [18] proposed a deep learning model based on Auto Encoder. They used NSL-KDD to investigate the self-taught learning model (STL). The model is made up of two fundamental process classifications. The first step in the compact attribute representation process is to train a dataset with unlabeled data. The second process is to train the learning representation features with labeled data and to implement the classification of IDS tasks. In the experiment, STL was used in two, five, and twenty-three classes. According to the results, STL achieved an accuracy of 88.39%, while the 5-class classification achieved an accuracy of 79.10%.

A deep learning model was based on the combination of Deep Belief Networks (DBNs) and probabilistic neural

networks [19]. DBN is responsible for converting low-dimensional representations to non-linear representations while retaining the important characteristics of raw data. They optimize hidden layer learning using particle swarm optimization. Additionally, Probabilistic Neural Network (PNN) makes use of final classification techniques for IDS detection. As demonstrated in their experiment, DBN-PNN achieved an accuracy of 93.25%. Additionally, DBN-PNN outperformed previous works that combined Principal Component Analysis (PCA) and Probabilistic Neural Networks (PNN).

A study proposed another deep learning model for the IDS task based on a Deep Belief Network (DBN) [20][21]. This model incorporates two critical processes: 1) they learned layer by layer using a restricted Boltzmann Machine (RBM), and 2) they derive the hidden layer vector from the visible layer vector. The hidden layer representation is the vector manifest for the following layer. The two processes combine backpropagation networks generated by the final RBM method and use the output vector generated by RBM as an input vector. The DBM model achieves a measurement accuracy of 95.25%. This results in a performance advantage of 89.07% over backpropagation and 91.36% over SVM.

DNN is an acronym for Deep Neural Network, which is considered suitable for use in IDS networks [22]. The DNN algorithm is a representation of an auto encoder with four hidden layers and one hundred hidden units. They use Rectified Linear Units (ReLU) to activate the hidden layer. ReLU classifies activation functions that are not linear. This activation function is intended to improve the algorithm's performance when performing complex classification tasks. The adaptive moment mechanism was used in this study to reach the stochastic optimizer. As demonstrated in the experiment, DNN achieved a measurement accuracy of 99%.

A novel model for detecting IDS networks using Convolutional Neural Networks (CNN) has been proposed [23]. The CNN model is well-suited to address a variety of image processing-related issues. In this IDS detection case, the author assumed that the image processing problem is similar to the IDS problem in terms of data vector dimension. CNNs are a subclass of feedforward neural networks that employ convolutional processes to condense large amounts of dimensional data into representative vectors. This work, which employs a CNN model, asserts that the model was successful in improving the imbalanced dataset and that the model not only reduced the false alarm rate but was also useful in enhancing the class's accuracy even when the sample size was small. As their experiment report indicates, CNN achieves an accuracy of 79.48% in KDD-NSL. It outperforms several conventional machine learning techniques that have been proposed in previous works.

GAN (Generative Adversarial Network) and AE were used on NSL-KDD, a novel IDS detection model [24]. When they applied a semi-supervised model, they reduced the time and effort required to manually label the labeled data and increased the effectiveness of IDS malicious detection without labeled data. Using GANs and AEs to improve IDS detection on NSL-KDD datasets, even with only 0.1% of the datasets that had labeled data, was a successful experiment report.

The Long Short-Term Memory (LSTM) is a subclass of feedforward neural networks with sequential aspect mechanisms [25]. It is a recurrent neural network enhancement. This year, LSTM is being considered as a possible model for an IDS network, such as the so-called DL-IDS [26]. DL-IDS has an accuracy rate of 98.67%, according to an experiment on Hybrid PCA/LSTM [26]. PCA is responsible for reducing raw data attack dimensions, while LSTM is tasked with classifying network attacks. They report that PCA-LSTM achieves 99.45% accuracy in binary class and 99.39% accuracy in multiclass. LSTM performance was improved by reducing the number of dimensions in the PCA model. They also proposed mutual information (MI) and LSTM in their research. It has a 96.24% binary class accuracy and a 95.56% multi-class classification accuracy.

III. MATERIAL AND METHOD

This study considers using NSL-KDD datasets to assess the efficacy of SDAE KNN, SVM, and Decision Tree variants. The datasets are widely used in IDS detection research. The detailed explanation and representative datasets are provided below.

A. NSL-KDD datasets explanation

NSL-KDD is an improved version of the KDD99 datasets. The datasets are widely used in the benchmarking mechanism of many IDS network detection systems. Furthermore, NSL-KDD improves some shortcomings in the original KDD99 datasets, such as the lack of repetition and replication in test and train records, which influences the bias of the classifier function against frequent samples. The dataset was created for free use by the Canadian Cybersecurity Institute [27]. The datasets are divided into training and testing configurations, which are denoted as KDDTrain+ and KDD_{Test+}, respectively, with a total of 125973 training records and 22544 testing records. Begun in the KDD_{Test+} recognized with additional 17 attack categories, in which it is not integrated into KDDTrain+, the researchers aim to achieve a classification result fairly, and thus removing 3751 categories was considered necessary. Furthermore, the KDDTest+ was 22544 - 3751 = 18793. Table 1 shows the detailed characteristics of the KDDTrain+ and KDDTest+. NSL-KDD, including the zf (f=1,2,3,4,5,..41) feature, which includes three symbolic attributes and 38 continuous attributes. The NSL-KDD datasets are divided into four attack class categories, as described below:

- Denial of Service (DoS): A DoS attack is when someone tries to make it impossible for people to get to a network service, server, or other services by flooding the internet with a lot of traffic. In a DoS attack, a server or network service can be slowed down or shut down by someone else.

- Root to Local (R2L): R2L attacks send remote packets that are not real to a server or computer system to get into the server or computer system without permission.
- User to Root (U2R): It is a group of attacks to get into the "root" area of a computer. In this example, the hacker finds out the system's flaw and logs in as a normal person.
- Probe: It is an attack category that can get information about networks and security management systems without being under the control of anyone.

Table 1 summarizes each attack category in detail. This follows the explanation in the previous text.

Table 1. NSL-Kdd datasets characteristics

NSL-KDD	TOTAL RECORD	NORMAL RECORD	DOS RECORD	PROBE RECORD	R2L RECORD	U2R RECORD
KDD_{Train+}	125973	67343	45927	11656	995	52
KDD_{Test+}	18793	9710	5741	1106	2199	37

B. Data Pre-processing

The goal of data pre-processing is to calculate data into a standard process so that it can be properly routed to the next stage section. It also ensures that the feature characteristic can be recognized by the machine learning algorithm. To achieve the goal, the pre-processing process is divided into three sections: data normalization, outliers data analysis, and dimensional data transformation using one-hot-encoding.

- **Removing outlier**: A value in the NSL-KDD is inconsistent. Outliers frequently use this term to describe this problem. Before the normalization of the data step, it has an essential procedure. In addition, outliers may have an impact on the proposed model of malicious detection, which could result in incorrect detection. We considered using Median Absolute Deviation Estimator (MADE), a technique whose working mechanism is represented in the following equation:

$$MADE=P*med(Z_{fj} - |med(Z_{fj})|)$$

- **Data normalization:** As part of the normalization process, the min-max method is used to calculate the Z_{fj} numerical attribute in the range of 0-1 with the following equation:

$$\tilde{z}_{fj} = \frac{z_{fj} - min(z_f)}{max(z_f) - min(z_f)}$$

- **One-hot-encoding:** Protocol model, service, and flag are three special feature characteristic attacks that necessitate a specific method of handling (z2, z3, z4). To convert them into a numeric number, the one-hot-encoding method is required. Every categorical feature, in particular, was demonstrated with a binary number. For example, protocol type is represented by three category attributes: udp, icmp, and tcp. The one-hot-encoding is in charge of the transformation into binary vector space, such as (1.0.0), (0.1.0), and (0.2.0). (0.0.1). The conversion process into a one-hot-encoding vector was also used for service and flag features with z3 and z4 symbol representation. The total number of feature attack characteristics in 41 features was computed into 122 dimensional features, which consisted of 84 dimensional features with binary class and 30 continuous values.
- **Dimensional reduction using SDAE:** SDAE is a subclass of auto encoder (AE) neural network, in which the AE takes the input and transforms it into hidden layer representation using a deterministic mechanism, while the denoising autoencoder is in charge of extracting the input's missing representation layer [28]. This model aims to address the auto encoder problem, which is difficult to train in deep learning models in order to detect unsupervised learning processes that map feature inputs into middle process representations. According to the literature, some versions of autoencoders have been proposed and have demonstrated tremendous achievement in the field of computer science research [29]. Furthermore, a class denoising autoencoder can be stacked to compute a deep layer, as seen in high-level classes where it is known as stack denoising autoencoder. SDAE, in particular for the learning mechanism, uses regularization to address the optimization problem.

$$\min_{W_l,b_l} ||X_{corrupted\_input} - X_{output}||_F^2 + \lambda \sum_l (\|W_l\|_F^2 + \|b_l\|_2^2)$$

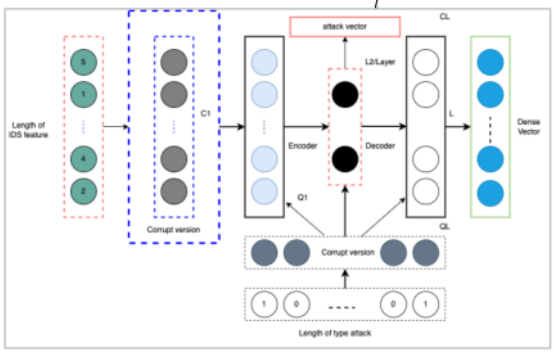

Fig. 3 SDAE Dimentional reduction framework

C. IDS Detection Classifier

This research considered incorporating four traditional classifier algorithms to observe the performance of the model. The dimensional reduction using SDAE integrated into Naive Bayes, KNN, Decision Three, and SVM. The basic mechanism of the algorithm is explained below.

- Naive Bayes

When dealing with binary (two classes) or multiclass classification problems, the Naive Bayes (NB) algorithm is the go-to choice. Binary or categorical input values make the technique easier to understand. Naive Bayes (also known as idiot Bayes) is a type of probability distribution that is simplified to make the calculation of the probabilities for each hypothesis tractable. To save time, rather than attempting to calculate the values of each attribute value $P(1)$, $P(2)$, and $P(3)|h)$, it is assumed that they are conditionally independent given the target value and the values are calculated as $P(d1|h) * P(d2|H)$ and so on.

- K-nearest neighborhood (KNN)

It is possible to use KNN, one of the simplest supervised machine learning algorithms, to predict the class of a particular data sample by considering "feature similarity." To identify a sample, it calculates its distance from the other samples in the neighborhood. The model's performance can be affected by the parameter k in the KNN algorithm. At very small k values, the model may be subject to over-fitting problems. The sample instance may be incorrectly categorized if a large number of k values are selected [28][29][30].

- Decision Tree

A Decision Tree (DS Tree) is a fundamental supervised machine learning algorithm that can be applied to both classification and regression problems on a given dataset (rules). Nodes, branches, and leaves make up the tree-like structure of the model. Each node is a feature or an attribute. Each leaf on the tree represents a possible outcome or classification, while the branch represents a rule or decision. To prevent over-fitting, the decision tree algorithm automatically selects the best features for creating a tree and then performs pruning operations to remove irrelevant branches from the tree. These three decision tree models are the most widely used: CART, C4.5, and ID3 [31][32].

- Support Vector Machine (SVM)

Using the SVM, a margin-based classification method, an optimum hyperplane is created that can effectively distinguish between the different classes as much as possible, following the principle of structural risk minimization [28]. As a result, SVM has a powerful generalization capability and is resistant to overfitting issues. Furthermore, SVM can deal with non-linear classification problems by selecting kernel functions to map the original feature space to some high-dimensional feature spaces with linearly separable instances.

D. Hybrid SDAE with Naive Bayes, KNN, Decision Tree, and SVM

Our study considers implementing SDAE and the popular traditional machine learning approach. It is a very important approach to observe the effectiveness level of several combinations between them. The schematic of the hybridization scheme can be seen in Figure 4 below. Our experiment consists of several evaluation processes, including multi-class and binary-class using confusion matrix, accuracy, recall, F1-measure, and precision. The multi-class experiment consists of 5 possibility conditions categories: normal, DoS, Probe, U2R, and R2L; while the binary class consists of 2 conditions: normal and anomaly.

We compared 4 traditional machine learning models including KNN, Naive Bayes, Decision Tree, and SVM. Then, they would be integrated into dimensional reduction based on SDAE respectively. SDAE is the enhancement of the Auto Encoder model. The advantage of variant Auto Encoder is that it is useful in feature extraction mechanisms. It is also a categorical modern deep machine learning. Our schematic training process divided the NSL-KDD into 30% and 70%. This schematic training ratio has been conducted by the majority of researchers in IDS detection.

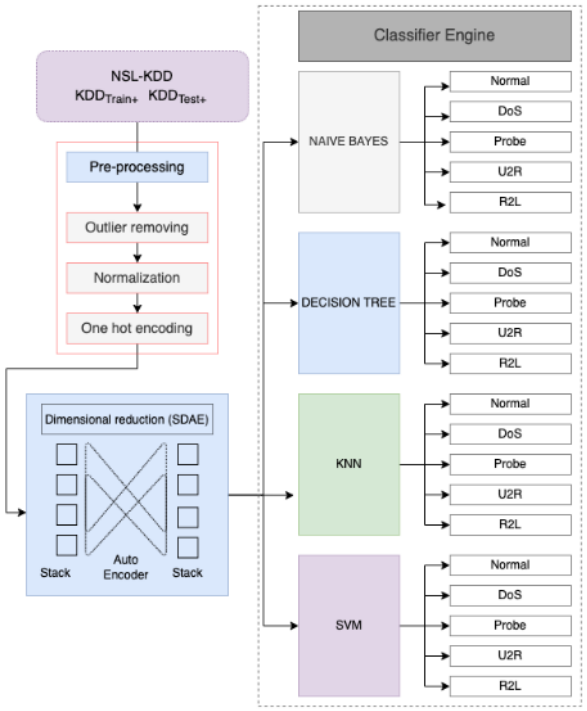

Fig 4. Detail hybridization model and experiment scenario

E. Evaluation Metrics

For example, TP represents the true positive rate, which indicates the number of abnormal samples that tested positive (accurate detection); TN represents the true negative rate, which indicates the number of normal samples that tested negative (accurate detection); FP represents the false positive rate, which represents how many abnormal samples tested positive (inaccurate detection); and FN represents the false-negative rate, which represents how many abnormal samples tested negative (accurate detection) (incorrect detection).

Accuracy is defined as the ratio of correctly classified samples to all samples in the testing set, expressed in percentage. Precision is defined as the ratio of correctly classified samples to the total number of TP and FP samples

in the testing set, expressed in percentage. The recall ratio is the ratio of the number of TP samples to the total number of TP and FN samples. When it comes to the time to compute the F1- score, it is calculated using the weighted average of precision and recall.

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

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

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

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

F. Result and analysis

The result of dimensional reduction using SDAE can be seen in Fig. 5 below. The dark colors represent values that are almost similar to the actual values, while the bright ones represent values that are very different from the actual values. Then, the output from dimensional reduction resulting from SDAE would be integrated into 4 machine learning categories.

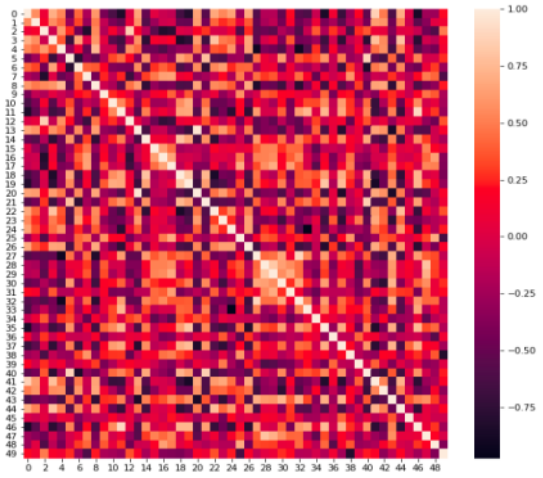

Fig 5. SDAE training result of NSL-KDD

The evaluation metrics include accuracy, precision, recall, and F1 as shown in Table 2. The experiment of our model consisted of 2 classes which were multi-class and binary class, in which binary class only detected an anomaly and normal detection, while multi-class involved 5 categories condition including "Normal", "DoS", "Probe", "R2L", and "U2R".

As shown in Table 3 and 4, the enhancement of dimensional reduction using SDAE succeeded to increase the effectiveness of traditional machine learning in IDS detection. The hybridization between SDAE and KNN model achieved an accuracy of 79.8% when compared with KNN without SDAE that only achieved 77.9%. The hybridization between SDAE and Naive Bayes also achieved better performance over the traditional Naive Bayes without SDAE with tremendous results in 80.5% compared to that of previous work results with 76.3%. Another successful model using a Decision Tree combined with SDAE achieved an accuracy of 83.4%, while the one without SDAE reached an accuracy of 82.9%. Our experiment report shows that SDAE and SVM achieved the best performance in 84.1% whereas the traditional SVM only achieved an accuracy of 80%.

The multi-class training result shows that the combination of SDAE with 4 machine learning also reached better performance over traditional machine learning. The hybridization among SDAE and KNN reached an accuracy of 78.1%, while KNN without SDAE only achieved 75%. The novel hybridization between SDAE and Naive Bayes achieved better performance in 78.7% over traditional Naive Bayes that only reached 77.8%. Another hybridization model between Decision Tree and SDAE showed better performance in 82.8%. This achievement was 2% higher than the traditional Decision Tree that only reached 80.1%. The best achievement in our experiment was reached by the hybridization between SDAE and SVM with an accuracy of 83.3%. It means that SDAE and SVM successfully increased the effectiveness level in IDS detection by more than 3% compared to the traditional SVM that only employed pre-processing process.

Our study also applied a confusion matrix to detect the effectiveness of our model. The confusion matrix was tried in each hybridization model and evaluated based on the multi-class and binary class classification approach. The binary class is shown in Fig. 6 to 13, while the multi-class classification can be seen in Fig. 14 to 21. Fig 6 to 13 demonstrated the involvement of SDAE, showing success in reducing misclass detection in every hybridization scenario including SDAE with KNN, Naive Bayes, Decision Tree, and SVM. Hybridization between SDAE and KNN could increase accuracy detection by 81% from 79%. The combination between SDAE and Naive Bayes achieved 82.9% while traditional pre-processing and Naive Bayes only reached 81.7%. The combination between SDAE and Decision Tree showed better performance over previous work with KNN and Naive Bayes in which SDAE and Decision Tree reached 85.5% while the traditional Decision Tree and pre-processing only reached 82.1%. Meanwhile, the hybridization between SDAE and SVM has become the best performance with an accuracy of 86.2%. The traditional pre-processing and SVM reached 82.1%. The employment of SDAE proved more effective in every hybridization scenario in multi-class classification. This model is also effective to detect 9341 normal network traffic with miss class detection in 946, and correct anomaly detection in 7274 with 1704 miss class detection.

Table 3. Comparison result on binary class measurement

Evaluation result on binary classification				
	Accuracy	Precision	Recall	F1
SDAE & SVM	84.1%	85.6%	83.1%	84.3%
SDAE & DS Tree	83.4%	83.4%	79.6%	81.4%
SDAE & NB	80.5%	81.8%	78.9%	80.3%
SDAE & KNN	79.8%	81.1%	74.1%	77.4%
Pre-processing & SVM	80.7%	81.9%	78.7%	80.2%
Pre-processing & DS3	82.9%	83.3%	81.2%	82.2%
Pre-processing & NB	76.3%	77.6%	73.8%	75.6%
Pre-processing & KNN	77.9%	78.3%	75.8%	77.0%

Table 4. Comparison result on multi-class measurement

Evaluation result on multi-classification				
	Accuracy	Precision	Recall	F1
SDAE & SVM	83.3%	85.1%	81.6%	83.3%
SDAE & DS Tree	82.8%	84.3%	80.8%	82.5%
SDAE & NB	78.7%	80.1%	76.1%	78.0%
SDAE & KNN	78.1%	79.7%	75.9%	77.7%
Pre-processing & SVM	80.0%	82.1%	77.8%	79.8%
Pre-processing & DS3	80.1%	82.7%	76.9%	79.6%
Pre-processing & NB	77.8%	79.1%	75.1%	77.0%
Pre-processing & KNN	75.6%	77.1%	72.3%	74.6%

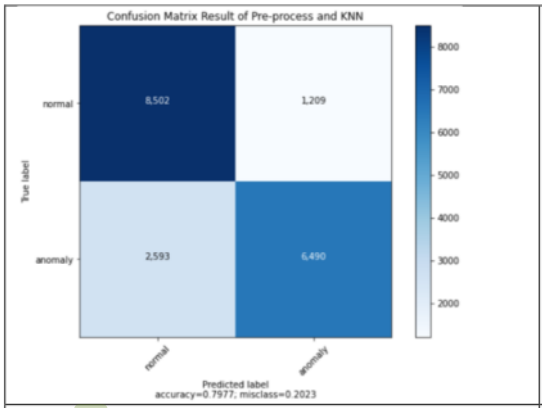

Fig 6. Confusion matrix of pre-processing and KNN in the binary class

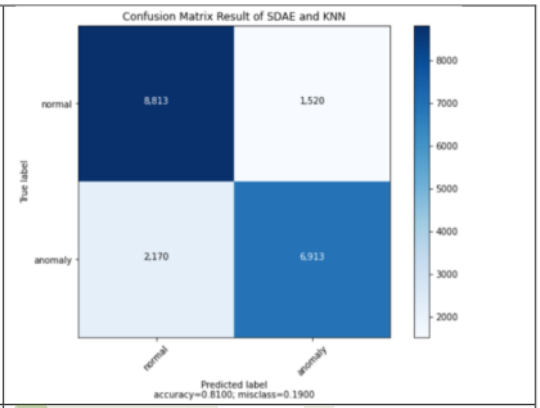

Fig 7. Confusion matrix of SDAE and KNN in the binary class

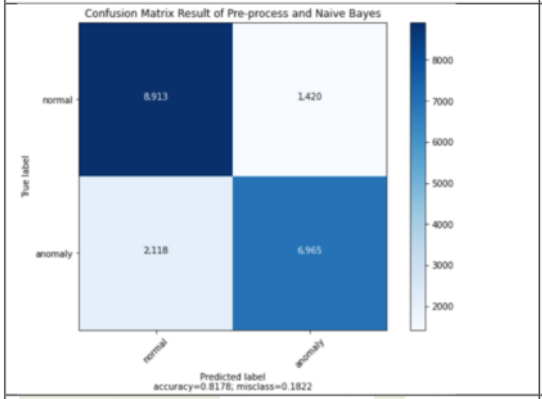

Fig 8. Confusion matrix of pre-processing and Naive Bayes in the binary class

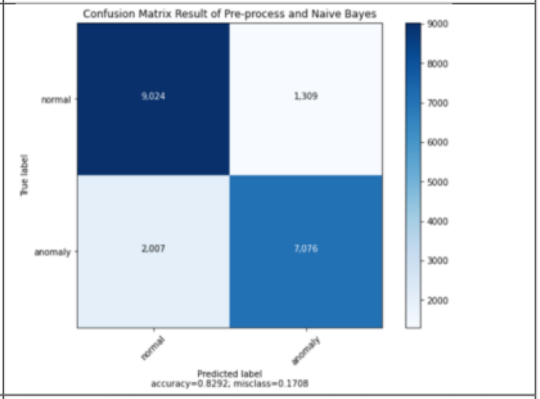

Fig 9. Confusion matrix of SDAE and Naive Bayes in the binary class

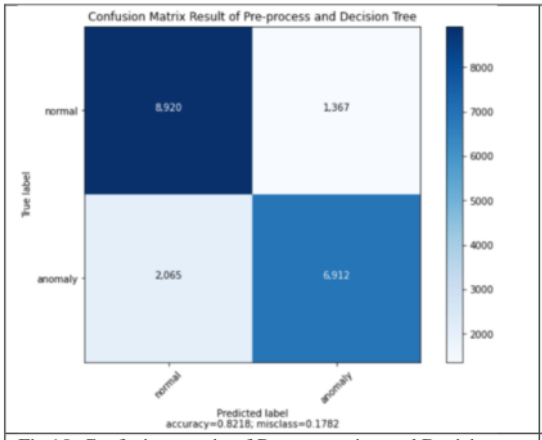

Fig 10. Confusion matrix of Pre-processing and Decision Tree in the binary class

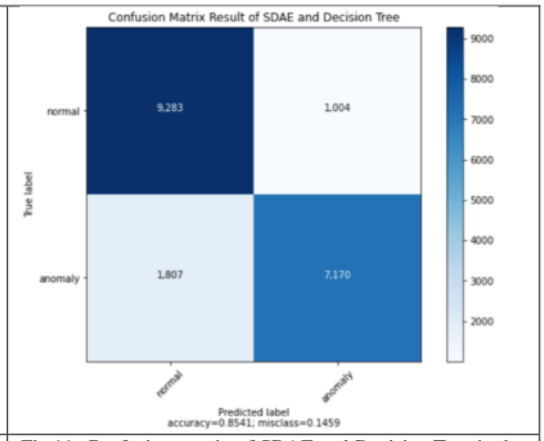

Fig 11. Confusion matrix of SDAE and Decision Tree in the binary class

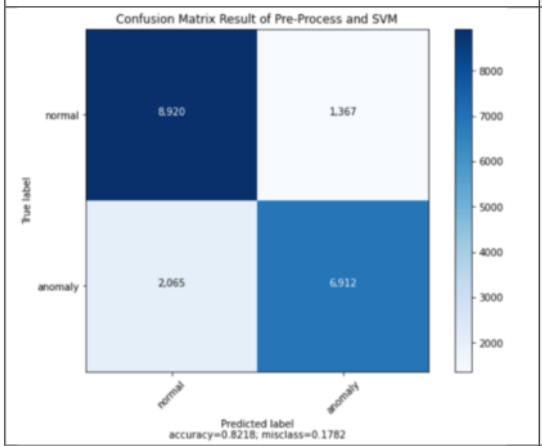

Fig 12. Confusion matrix of Pre-processing and SVM in the binary class

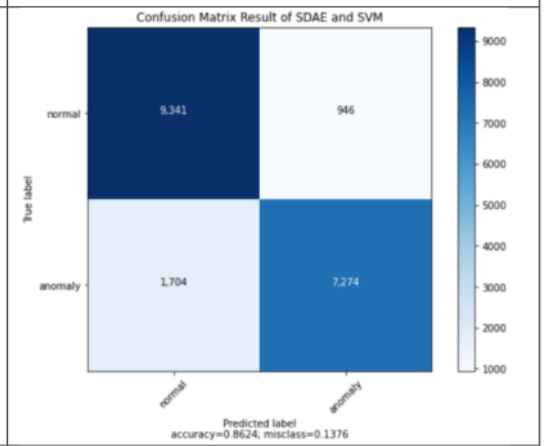

Fig 13. Confusion matrix of SDAE and SVM in the binary class

The experiment report based on the confusion matrix on multi-class classification is shown in Fig. 14 to 21. Each figure shows that SDAE could reduce miss class detection. The involvement of SDAE supported KNN to enhance the accuracy level in confusion matrix evaluation by 74%, while the traditional KNN and pre-processing only reached 72%. The combination between SDAE and Naive Bayes was also successful to increase performance in multi-class IDS detection in which this model achieved an accuracy of 79.9% compared to Naive Bayes and pre-processing that reached an accuracy of 77.9%. The Decision Tree that applied SDAE was also successful to reduce miss classification and increase accuracy in confusion matrix evaluation that achieved 83.2% whereas the Decision Tree without SDAE only reached 82%. Another hybridization model involving SDAE and SVM, evaluated using a confusion matrix, reached the best performance over the previous hybridization approach. SDAE-SVM could reduce miss classification and increase accuracy performance by 87% and achieve an accuracy of 84% in pre-processing and SVM only.

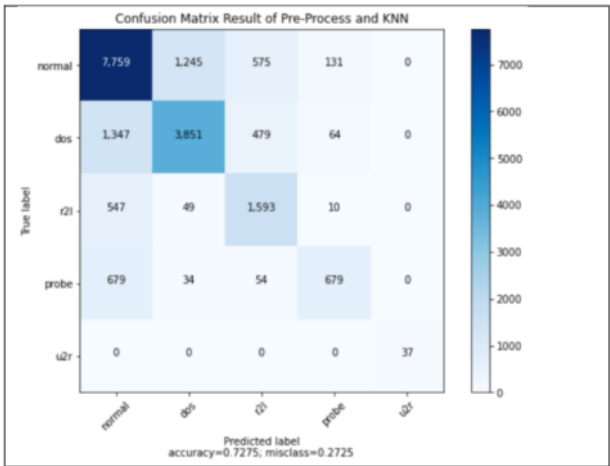

Fig 14. Confusion matrix of Pre-processing and KNN in multi-class

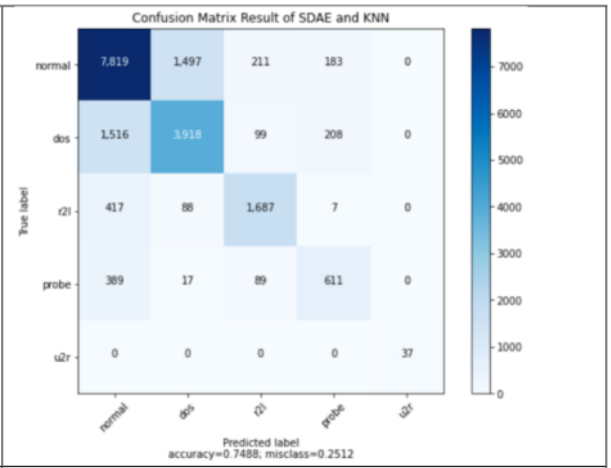

Fig 15. Confusion matrix of SDAE and KNN in multi-class

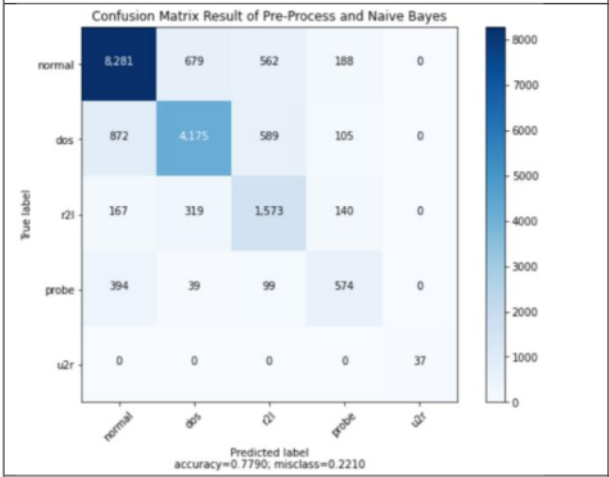

Fig 16. Confusion matrix of Pre-processing and Naive Bayes in multi-class

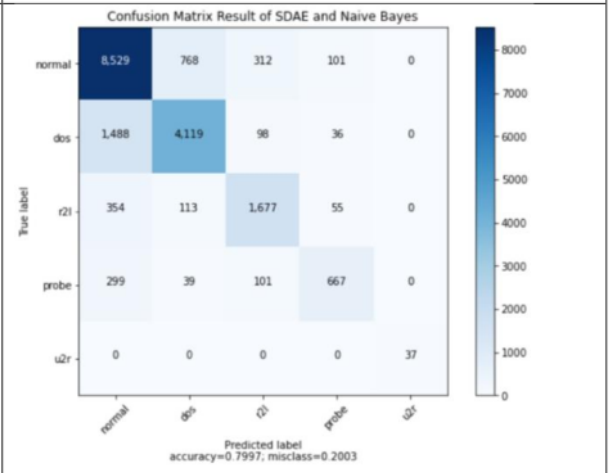

Fig 17. Confusion matrix of SDAE and Naive Bayes in multi-class

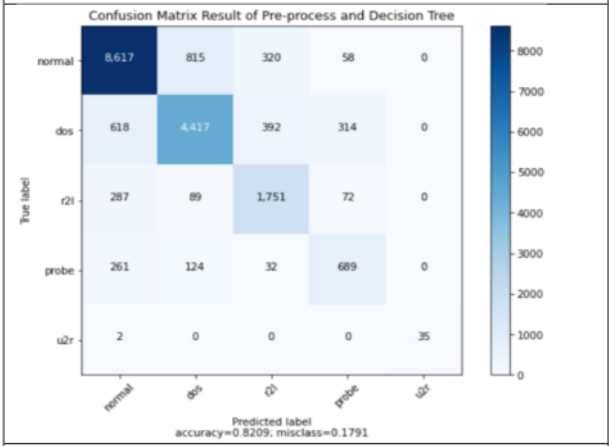

Fig 18. Confusion matrix of Pre-processing and Decision Tree in multi-class

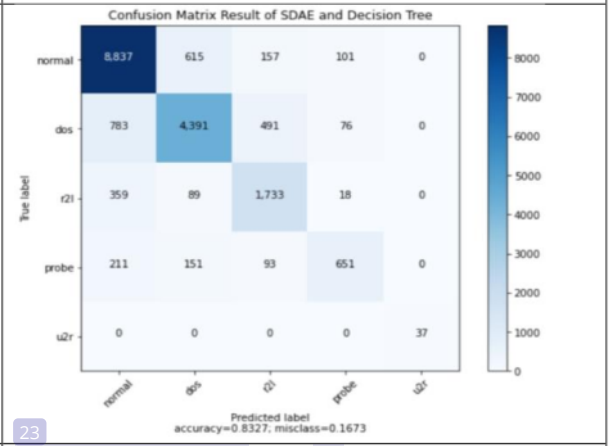

Fig 19. Confusion matrix of SDAE and Decision Tree in multi-class

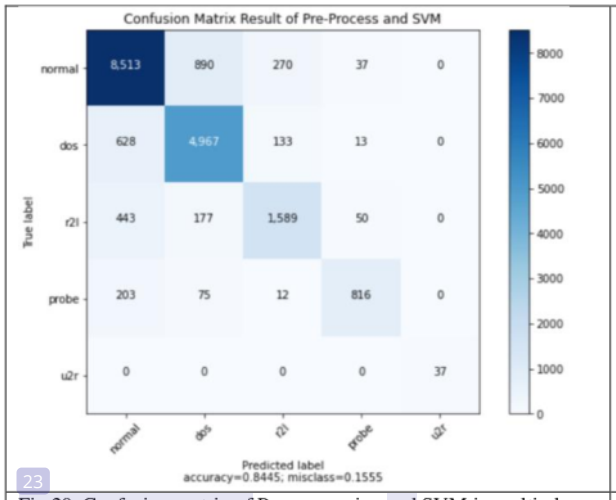

Fig 20. Confusion matrix of Pre-processing and SVM in multi-class

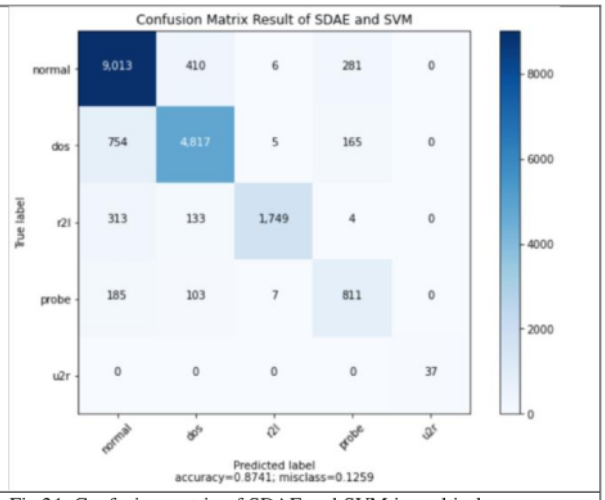

Fig 21. Confusion matrix of SDAE and SVM in multi-class

The comparison result over the previous state-of-the-art has been conducted on this study. The competitor used several novel methods based on statistical and deep learning approaches, for instance, the hybridization of statistical models with machine learning, the combination between CNN and LSTM, LSTM and Mutual information, and LSTM and PCA. The comparison is shown in Table 3.

Table 3. Comparison Result Over State-Of-The-Art

No	Model	Accuracy
1	SDAE & SVM (our model)	**84.1%**
2	SDAE & Decision Tree (our model)	83.4%
3	SDAE & Naive Bayes (our model)	80.5%
4	SDAE & KNN (our model)	79.8%
5	CNN & LSTM (BAT) [33]	**84.25%**
6	Statistic & ML [34]	83.65%
7	LSTM & PCI [26]	82.4%
8	LSTM & MI [26]	81.8%

IV. Conclusion

This present study considers enhancing dimensional reduction using a variant of auto encoder based on SDAE. It is found that this model is useful to improve the traditional machine learning work. SDAE is also suitable to reduce miss classification in popular traditional machine learning such as KNN, Naive Bayes, Decision Tree, and SVM. The best combination in our experiment was achieved by SDAE and SVM compared over the other models such as Decision Tree (the second-best achievement), Naive Bayes, and KNN.

SDAE was also successful in increasing the effectiveness of classification mechanisms in machine learning especially in IDS detection even when compared to modern machine learning approaches such as deep learning based on CNN and LSTM in binary and multi-class classification methods.

There are some challenges in future research, in that SDAE is possible to be integrated with modern deep learning such as MLP, LSTM, CNN, and GAN to reduce miss class prediction and increase the correct value prediction. Our model that is developed using traditional machine learning is highly possible to be improved with an ensemble learning approach.

Acknowledgment

References

[1] B. Zarpelão, R. Miani, … C. K.-J. of N. and, and undefined 2017, "A survey of intrusion detection in Internet of Things," *Elsevier*, 2017.

[2] K. N. L. biswanath Mukherjee, L. Todd Heberlein, "Network Intrusion Detection," *IEEE Network*, 1994.

[3] S. Wagh, A. ali shah, S. Kishor Wagh, V. K. Pachghare, and S. R. Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," *International Journal of Computer Applications*, vol. 78, no. 16, pp. 975–8887, 2013.

[4] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches Emulated Monitoring Systems View project Deep Learning View project Survey on SDN based network intrusion detection system using machine learning approaches."

[5] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 1, 2020.

[6] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "IDS - attention : an efficient algorithm for intrusion detection systems using attention mechanism," *Journal of Big Data*, 2021.

[7] H. Zhang, "Design of intrusion detection system based on a new pattern matching algorithm," *Proceedings - 2009 International Conference on Computer Engineering and Technology, ICCET 2009*, vol. 1, pp. 545–548, 2009.

[8] C. Yin, "An Improved BM Pattern Matching Algorithm in Intrusion Detection System," *Applied Mechanics and Materials*, vol. 148–149, pp. 1145–1148, 2012.

[9] D. E. Denning, "An Intrusion-Detection Model," *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, vol. 13, no. 2, pp. 222–232, 1987.

[10] M. Pervez, D. F.-T. 8th I. C. on, and undefined 2014, "Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs," *ieeexplore.ieee.org*, 2015.

[11] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based

network intrusion detection systems," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 38, no. 5, pp. 649–659, 2008.

[12] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," *International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*, pp. 92–96, Mar. 2015.

[13] B. Ingre, A. Yadav, and A. K. Soni, "Decision Tree Based Intrusion Detection System for NSL-KDD Dataset," *Smart Innovation, Systems and Technologies*, vol. 84, pp. 207–218, 2017.

[14] N. Rusk, "Deep learning," *Nature Methods*, vol. 13, no. 1, p. 35, 2015.

[15] Hanafi, N. Suryana, and A. S. B. H. Basari, "Deep learning for recommender system based on application domain classification perspective: A review," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 14, 2018.

[16] Hanafi, A. Pranolo, and Y. Mao, "Cae-covidx: Automatic covid-19 disease detection based on x-ray images using enhanced deep convolutional and autoencoder," *International Journal of Advances in Intelligent Informatics*, vol. 7, no. 1, pp. 49–62, 2021.

[17] Hanafi and B. M. Aboobaider, "Word Sequential Using Deep LSTM and Matrix Factorization to Handle Rating Sparse Data for E-Commerce Recommender System," *Computational Intelligence and Neuroscience*, vol. 2021, no. 1, 2021.

[18] A. Javaid, Q. Niyaz, W. Sun, M. A.-E. T. on, and undefined 2016, "A deep learning approach for network intrusion detection system," *eprints.eudl.eu*, 2016.

[19] G. Zhao, C. Zhang, L. Z.-2017 I. International, and undefined 2017, "Intrusion detection using deep belief network and probabilistic neural network," *ieeexplore.ieee.org*, 2017.

[20] F. Qu, J. Zhang, Z. Shao, S. Q.-P. of the 2017 V. international, and undefined 2017, "An intrusion detection model based on deep belief network," *dl.acm.org*, pp. 97–101, Dec. 2017.

[21] M. Alom, … V. B.-2015 N. A., and undefined 2015, "Intrusion detection using deep belief networks," *ieeexplore.ieee.org*.

[22] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," *2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017*, pp. 313–316, Mar. 2017.

[23] K. Wu, Z. Chen, and W. Li, "A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018.

[24] K. Hara and K. Shiomoto, "Intrusion Detection System using Semi-Supervised Learning with Adversarial Auto-encoder," *Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020*, 2020.

[25] S. Hochreiter and J. Urgen Schmidhuber, "Lstm," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[26] F. E. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, 2021.

[27] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*, no. July, 2009.

[28] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, no. 1, 2014.

[29] R. Taguelmimt and R. Beghdad, "DS-kNN: An intrusion detection system based on a distance sum-based K-nearest neighbors," *International Journal of Information Security and Privacy*, vol. 15, no. 2, pp. 131–144, 2021.

[30] S. Choi, "Combined kNN classification and hierarchical similarity hash for fast malware detection," *Applied Sciences (Switzerland)*, vol. 10, no. 15, pp. 1–16, 2020.

[31] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for internet-of-things networks," *Future Internet*, vol. 12, no. 3, pp. 1–14, 2020.

[32] K. Rai, M. S. Devi, and A. Guleria, "Decision Tree Based Algorithm for Intrusion Detection," *International Journal of Advanced Networking and Applications*, vol. 07, no. 04, pp. 2828–2834, 2016.

[33] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020.

[34] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, 2020.

An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning

ORIGINALITY REPORT

15%	7%	12%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mohammad Mehedi Hassan, Abdu Gumaei, Ahmed Alsanad, Majed Alrubaian, Giancarlo Fortino. "A hybrid deep learning model for efficient intrusion detection in big data environment", Information Sciences, 2020 Publication	2%
2	Yadala. Prabhu Kumar, Burra. Vijaya Babu. "A Comprehensive Analysis on Predictor Models for Intrusion Detection using Mining And Learning Approaches", 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022 Publication	1%
3	Jie Gu, Shan Lu. "An effective intrusion detection approach using SVM with naïve Bayes feature embedding", Computers & Security, 2020 Publication	1%
4	Submitted to Universitas Muhammadiyah Yogyakarta Student Paper	1%

5	Donald J. Norris. "Machine Learning with the Raspberry Pi", Springer Science and Business Media LLC, 2020 Publication	1 %
6	inass.org Internet Source	<1 %
7	journalofbigdata.springeropen.com Internet Source	<1 %
8	Souradip Roy, Juan Li, Yan Bai. "A Two-layer Fog-Cloud Intrusion Detection Model for IoT Networks", Internet of Things, 2022 Publication	<1 %
9	Mosleh M. Abualhaj, Ahmad Adel Abu-Shareha, Mohammad O. Hiari, Yousef Alrabanah, Mahran Al-Zyoud, Mohammad A. Alsharaiah. "A Paradigm for DoS Attack Disclosure using Machine Learning Techniques", International Journal of Advanced Computer Science and Applications, 2022 Publication	<1 %
10	Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Transactions on	<1 %

Emerging Telecommunications Technologies, 2020
Publication

11	Submitted to Symbiosis International University Student Paper	<1%
12	doctorpenguin.com Internet Source	<1%
13	"Advances in Brain Inspired Cognitive Systems", Springer Science and Business Media LLC, 2018 Publication	<1%
14	Submitted to University of Leeds Student Paper	<1%
15	Farrukh Aslam Khan, Abdu Gumaei, Abdelouahid Derhab, Amir Hussain. "TSDL: A TwoStage Deep Learning Model for Efficient Network Intrusion Detection", IEEE Access, 2019 Publication	<1%
16	aclanthology.org Internet Source	<1%
17	Submitted to iGlobal University Student Paper	<1%
18	Kehe Wu, Zuge Chen, Wei Li. "A Novel Intrusion Detection Model for a Massive	<1%

Network Using Convolutional Neural Networks", IEEE Access, 2018
Publication

19	Submitted to Universiti Teknologi MARA Student Paper	<1 %
20	Submitted to University of Teesside Student Paper	<1 %
21	Submitted to Brigham Young University Student Paper	<1 %
22	Emre Uzundurukan, Aysha M. Ali, Yaser Dalveren, Ali Kara. "Performance Analysis of Modular RF Front End for RF Fingerprinting of Bluetooth Devices", Wireless Personal Communications, 2020 Publication	<1 %
23	Li, Dan, Yuxun Zhou, Guoqiang Hu, and Costas J. Spanos. "Fault detection and diagnosis for building cooling system with a tree-structured learning method", Energy and Buildings, 2016. Publication	<1 %
24	Signals and Communication Technology, 2015. Publication	<1 %
25	sure.sunderland.ac.uk Internet Source	<1 %
26	ir.ia.ac.cn Internet Source	<1 %

27	www.researchgate.net Internet Source	<1%
28	Insoo Sohn. "Deep Belief Network based Intrusion Detection Techniques: A Survey", Expert Systems with Applications, 2020 Publication	<1%
29	link.springer.com Internet Source	<1%
30	Cosimo Ieracitano, Ahsan Adeel, Francesco Carlo Morabito, Amir Hussain. "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach", Neurocomputing, 2019 Publication	<1%
31	Nguyen Dat-Thinh, Ho Xuan-Ninh, Le Kim-Hung. "MidSiot: A Multistage Intrusion Detection System for Internet of Things", Wireless Communications and Mobile Computing, 2022 Publication	<1%
32	arxiv.org Internet Source	<1%
33	avis.ajou.ac.kr Internet Source	<1%
34	export.arxiv.org Internet Source	<1%

35	www.science.gov Internet Source	<1%
36	"Explainable Artificial Intelligence for Cyber Security", Springer Science and Business Media LLC, 2022 Publication	<1%
37	Feng Qu, Jitao Zhang, Zetian Shao, Shuzhuang Qi. "An Intrusion Detection Model Based on Deep Belief Network", Proceedings of the 2017 VI International Conference on Network, Communication and Computing - ICNCC 2017, 2017 Publication	<1%
38	Josy Elsa Varghese, Balachandra Muniyal. "An investigation of classification algorithms for intrusion detection system — A quantitative approach", 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017 Publication	<1%
39	Linbei Wang, Zaoyu Tao, Lina Wang, Yongjun Ren. "A Hybrid Intrusion Detection Model Based on Spatiotemporal Features", Journal of Quantum Computing, 2021 Publication	<1%
40	Xiaokang Zhou, Yue Li, Wei Liang. "CNN-RNN Based Intelligent Recommendation for Online	<1%

Medical Pre-Diagnosis Support", IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2020
Publication

41	ir.lib.uwo.ca Internet Source	<1%
42	papyrus.bib.umontreal.ca Internet Source	<1%
43	vdoc.pub Internet Source	<1%
44	www.hindawi.com Internet Source	<1%
45	Kaiyuan Jiang, Wenya Wang, Aili Wang, Haibin Wu. "Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network", IEEE Access, 2020 Publication	<1%
46	Sepp Hochreiter, Jürgen Schmidhuber. "Long Short-Term Memory", Neural Computation, 1997 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12