مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 123) 2024, pp. 73-87

Use of Singular Value Decomposition for a Deep Learning-Based Fast Intrusion Detection System

Inbithaq A. Shakir [(1)]
Department of Computer
College of Science, Mustansiriyah University,Baghdad,Iraq,
inbethaqahmed_2020@yahoo.com
Prof.Ahmed A. Al-fetouh Saleh [(2)]
Department of Information Systems, Faculty of Computer & Information Systems, MansouraUniversity, Mansoura, Egypt.
elfetouh@mans.edu.eg
Prof.Hazem M.El-Bakry[(3)]
Department of Information Systems, Faculty of Computer & Information Systems, MansouraUniversity, Mansoura, Egypt
helbakry1@hotmail.com

Abstract:
An artificial intelligence technique based on artificial neural networks for identifying risks. A range of professions, including the recognition of specific patterns or categories, have adopted deep learning methodologies. Data from intrusion detection assessments and security event monitoring were used to evaluate the network situation. The performance and accuracy of the detection must be improved. We decided to test a range of approaches utilizing an open data set in order to identify the best approach for intrusion detection. The current study aims to explore the possibility of using singular value decomposition (SVD) as a pre-processing step to reduce the dimensionality of the data. In addition to reducing the noise from the data, this pre-processing step reduces the dimensionality of the data to save time on calculations. The proposed strategy can help other currently used methods perform better. We test reduction strategies on the UNSW-NB15 dataset, and the outcomes are very positive.

Keywords: Intrusion detection, singular value decomposition (SVD),deep-learning, network security.

Introduction:

With the advancement of artificial intelligence (AI) capabilities, learning-based systems for identifying cyberattacks have advanced further and have produced noteworthy results in various studies. However, because assaults are always evolving, protecting IT systems from threats and illicit network activity is still exceedingly challenging. Due to frequent network intrusions and illegal activities, strong defenses and security considerations were given major attention in order to build a reliable solution [1]. Intrusion detection, which is generally used for tracking and locating intruders, is necessary for many network domains.

There are several problems with traditional intrusion detection models (IDS), including poor detection of unknown network threats, a high percentage of false alarms, and restricted analysis capabilities. Therefore, the main objective of research in this area is to develop a more accurate and quick-to-train intrusion detection model. generalization. Fewer resources are used since the classifier input needs a smaller feature set for ideal categorization. Due to the frequency and complexity of Internet attacks, system administrators now require a higher level of knowledge to effectively detect breaches. Due to their ability to automate this monitoring and analysis process, intrusion detection systems (IDS), which can be either software or hardware [1, 2]. Based on the data it has collected, the ID system decides if the behavior is normal or obtrusive. The two types of ID systems are misuse-based systems and anomaly detection systems. Misuse detection refers to intrusions that follow particular attack trajectories and make use of structural vulnerabilities. Techniques for identifying misuse have a good detection rate for known attacks but struggle to identify new attacks or even known attack variants. Systems for spotting anomalies try to replicate or learn typical or normative behavior as it is defined by the company's security policy. The likelihood of an intrusion increases with each significant deviation from this established routine [2,3].In the current study, we focus on preparing the data that will be assessed for intrusion detection and investigating a way to reduce the dimensionality of the data being fed into the network-based system without compromising the system's performance. In order to reduce the dimension, the singular value decomposition (SVD) method is applied [3]. Concepts from one of the informative approaches are used in this research. To reduce the size of the vectors, we employ singular value decomposition (SVD; more on this later). We test the proposed model using deep learning

on the UNSW-NB15 dataset to show the effectiveness of our methods, and we then test the proposed model without using elimination tactics [4],[5].The format of the paper Information about intrusion detection systems is provided; earlier works are in Section 2. Background information is in Section 3. Section 4 should include a suggested model. Discussions and experimental results are found in Section 5. Section 6 offers conclusions in the end.

Previous Studies: earlier research on actual security event analysis and deep learning-based intrusion detection [6]. These investigations are still restricted to particular test datasets like UNSW-NB15, despite having achieved notable achievements employing AI and SVD-based approaches.

Ashiku and C. Dagli [7] developed deep learning models for identifying and categorizing network risks in emerging systems networks (IDS). The proof focuses on how deep learning, also known a deep neural networks (DNNs), may enable accurate intrusion detection by training to recognize recognizable and distinctive network behavioral patterns, The performance was examined using the UNSW-NB15 dataset. The experimental findings showed a performance accuracy of 95.6%. **Mahalakshmi et al. [8]** The CNN deep learning model was used in the development of the IDS to increase the effectiveness of intrusion detection. The UNSW NB15 Dataset and CNN algorithm classification approach, with an accuracy of 93.5% .**Naseer et al. [9]** a variety of deep neural network designs, including CNNs, auto encoders, and RNNs, were devised, put into practice, and trained for intrusion detection. Both of NSLKDD's test datasets were used to evaluate these models after they had been trained on the NSLKDD training dataset,DCNN and LSTM models performed with an accuracy of 85% and 89%, respectively.**Wang et al. [10]** suggested a hierarchical intrusion detection system (HAST-IDS) that automatically learns network traffic features. The fundamental notion is that deep CNNs are used to initially learn the geographical characteristics of network traffic, and then LSTM networks are used to learn the temporal characteristics. Using ISCX datasets and DARPA, the experiments were carried out. **R.Vinayakumar et al. [11]**A hybrid intrusion detection system that can assess host- and network-level activity has been developed. It made use of a distributed deep learning model with DNN to instantly process and analyse huge amounts of data, including NSLKDD and UNSW-B15.**Khan et al. [12]** For effective network intrusion detection, we suggest a unique two-stage deep learning model built on stacked auto-

encoders and soft-max classifiers. NB15 datasets from UNSW 89.1% of the UNSW-NB15 dataset was successfully used in this investigation.

3-The Researcher' Work

We begin by introducing deep learning techniques and providing an overview of the SVD. For the suggested deep learning CNN system, we summarize our big data platform in the last section.

3-1 Deep learning

New methods in a number of sub-disciplines, such as image recognition, computer security, and speech recognition, has made the area of deep learning active. Due to the corresponding growth in data creation, the traditional deep learning algorithms employed in network security are increasingly failing to detect breaches in network systems. As a result, the most recent invention that attempts to examine information patterns with a view to detecting unwanted entrance into computer networks is big data analysis employing a deep belief system [13].Beyond machine learning applications where neurons are used as mathematical structures resembling human brain networks, deep learning has made significant strides in many fields in recent years and continues to do so in many other industries. Convolutional and recurrent models of deep neural networks are the most commonly utilized types.RNNs are a better option since they can learn using a variety of time-continuously changing aspects of data, while CNNs are often good at learning spatial features of data such as image processing. CNNs are designs that were created specifically to handle spatial data. CNNs are used in many different domains because of their awareness of the partially particular features of the input, specific local characteristics, and shared parameter schemes. In numerous disciplines, including image classification [11-14]

3-2 Convolution neural network model

Convolution neural networks (CNNs) are neural network designs that were created specifically to handle spatial data. Data from a 2D or 3D array, such as the pixel value of an image's information, makes up the input layer for CNN. Convolutional layers (Conv) and max pooling layers make up the foundation of CNN. Input is received as a unit by a Conv layer, which convolves it using filters to create continuing data that is transferred to the following layers.

The filters read the entire inputted data in a Conv layer by slicing and extracting the important features. Additionally, the scalar product between

each filter and the input chunk is calculated to accomplish convolution. The features that each filter extracts are combined into a new feature set known as the feature map [15]. The convolutional layer produces a feature map for each of the groups of filters it comprises and then aggregates the data from feature maps to produce data for output.The intended and implemented CNN consisted of an input layer, nine convolutional layers, six max-pooling layers, an output layer, and one fully connected layer. Eight incorrect ReLU layers were layered. Spread out one layer. and three substantial layers.

The input layer of the actual CNN is built dynamically. Because CNNs are frequently created to process 2D or 3D pixel data from the processing image, we must transform each pre-processed event profile row into a CNN. Therefore, we change each element of the incoming data. vector into a 2D array with N empty cells, where N = N. 0 is substituted for them in the 2D array. Afterward, based on the dimensions of the defined qualities, each layer of input can be examined [14].

4- Techniques for dimensionality reduction

The low-dimensional data representation of the initial data often solves the dimensionality curse problem and facilitates easy analysis, processing, and visualization. Dimensionality reduction strategies have advantages when used on datasets.

1. Reduction in the size of the dimensions and the data storage area. 2. The computation is quicker. 3. Repetitive, noisy, and irrelevant data can be removed. 4.The quality of the data can be raised. 5. improves accuracy and helps an algorithm run more effectively. 6. It improves output and streamlines categorization [16].

Since it enables the effective reduction of redundancy, the elimination of unnecessary data, and an improvement in the readability of findings, feature selection (FS) is regarded as a key technique in light of the constant production of data at an ever-increasing rate. Furthermore, feature extraction, which identifies the most distinct, perceptive, and condensed group of qualities, is used to improve the proficiency of data processing and storage.

4-1 Singular Value Decomposition (SVD)

The SVD technique locates and groups the dimensions with the largest inter-data point variation. It can give the best approximate representation of the original data points with fewer dimensions after identifying the largest variation. Because of this, SVD may be thought of as a great technique for

decreasing features in any dataset [16, 17], assuming X produces an m-n matrix.

The following concept is used to determine the top K single values:

1. The stake matrix U is orthonormal and contains m x k stacks. The dot product of any two stakes in this matrix, which each represents a unit vector, is the same.
2. The stake model V has n stakes and is orthonormal. V is a representation of the modified orthonormal rows of VT. In order of decreasing importance, the stakes are listed.
3. There are k elements in the diagonal matrix S. There is nothing that is not contained inside the principal diagonal. S elements are used to represent X's singular values.
4. Using the SVD components U, S, and V, a big matrix X can be divided into three equally large matrices.

$$X_{m\times n} = U_m \times kSk \times k(V_n \times k)T \quad \ldots (1)$$

One of the entering matrices, X, is used to obtain a k-low dimensionality via the SVD notion, which is demonstrated in Eq. (2). U, S, and VT are shortened forms of U, S, and VT, respectively. In this instance, Y just keeps the top k individual value

$$Y = U_k \times S_k \times V_k^T \quad \ldots (2)$$

This method is described in detail in Algorithm (1).

Algorithm (1). "Singular Value Decomposition"

Input: Standardized data

Output: Reduced features

Begin

1: calculate V V^T and V^T V.

2: Calculate the X matrix using Eq. (1).

3: Calculate the Y matrix using Eq. (2).

4: Diagonalize the data matrix.

5: Return (Reduced Features)

End.

5-Suggest model to classify data

The proposed system for threat detection based on artificial intelligence is described in this section's architecture. The system uses SVD together with data pretreatment mechanisms that enable the handling of very large-scale network events, in addition to deep learning approaches. It is necessary to perform the essential steps (data preparation, data splitting, feature reduction, classification, and evaluation) of the specified system design. The first step in data preparation is standardization. Second, the feature reduction procedure makes use of the singular value decomposition (SVD). These strategies aid in minimizing the number of features needed for the classification phase and aid in the selection of the most crucial ones. The third stage determines whether the network data flow is normal or abnormal using the proposed Network Intrusion Detection Convolutional Neural Networks (NIDCNN) model. Finally, the results of the suggested model were assessed using a range of metrics. The primary structure of the suggested system is shown in Figure 2. The data travel via the network is categorized once it has passed the aforementioned phases. This is where the proposed classification algorithm comes into play in determining this and helping to protect data security from any network intrusion. Because of how it is structured, the suggested system can quickly and accurately detect any anomalous movement. The proposed NIDCNN model consists of the following 27 layers.

Initial phase: loading the UNSW-NB15 dataset

The UNSW IXIA Perfect Storm tool The arriving network packets for the UNSW-NB 15 dataset were developed by Canberra's Cyber Range Lab to provide a blend of real-world contemporary everyday operations and synthetic current attack behaviors. Using the tcpdump program, 100 GB of unpasteurized communications were discovered (example: Pcap files). Nine different attack types can be used against UNSW-NB15, including DoS, Generic, Exploits, Shellcode, Reconnaissance, Backdoor, Worms, Analysis, and Fuzzers. Using the Intrepid and Dude programs, 12 strategies are constructed and 49 characteristics are produced [18].The NB15's characteristics are UNSW A CSV file contains a description of the features. The UNSW-NB15 data set is seen as a new standard for evaluating NIDSs and is thought to be more difficult than KDD99.

A second phase: dataset division

Hold-out validation was used to ensure proper generalization and avoid overtraining. Two subsets of the UNSW-NB15 dataset were created: one for training sets (70%) and one for testing sets (30%).

A third phase: pre-processing the UNSW-NB15 dataset

transform the raw dataset into a straightforward and effective format. It is therefore a time-consuming process with the main objective of producing a dataset that is trustworthy and appropriate for deep learning algorithms. In this case, the conventional scaler strategy is used for both procedures (training and testing).

A fourth phase: reduce features

It is also known as dimensionality reduction, and it involves reducing the number of features in a computation that uses a lot of resources without sacrificing crucial data.Fewer characteristics mean fewer variables, which facilitates faster processing by the computer. Feature extraction and feature selection are the two processes involved in feature reduction. There are several ways to reduce features. Using Singular Value Decomposition (SVD)

A fifth phase: Make an NIDCNN classification model

The data travel via the network is categorized once it has passed the aforementioned phases. Either it happens naturally or someone is trying to hack the network to get users' personal information. This is where the proposed classification algorithm comes into play in determining this and helping to protect data security from any network intrusion. Because of how it is structured, the suggested system can quickly and accurately detect any anomalous movement. The deep learning CNN technique model consists of the following 27 layers (see figure 1).consist from nine-layer Convolutional Neural Network (CNN),six layer maximum pooling eight layers of leaky ReLU, one layer flat and three Dense layer.

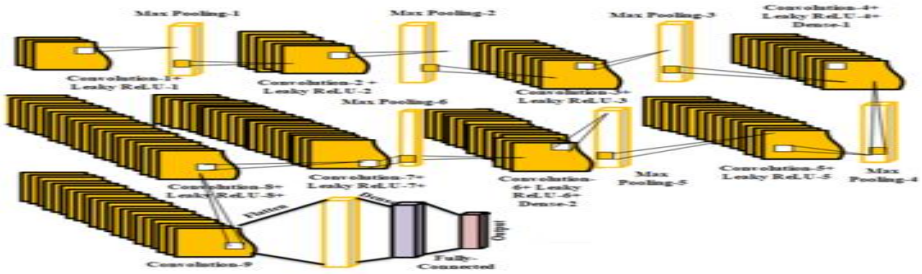

Fig.(1): CNN Technique

Therefore, the Deep Learning CNN Technique model represents the CNN technique as suggested in Figure 2. It consists of twenty-seven layers, each of Which performs its respective function.

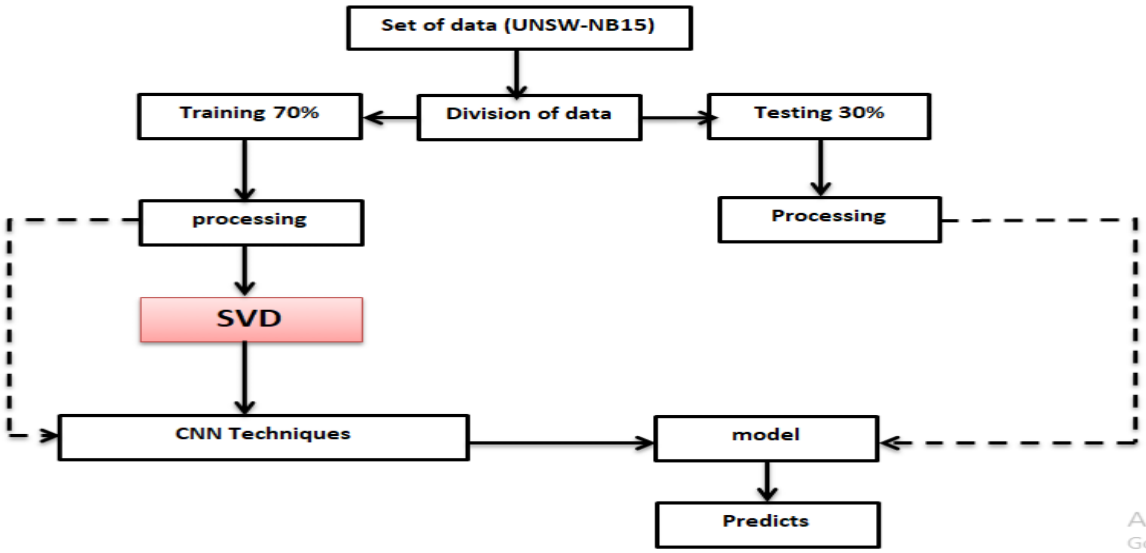

Fig.2.Deep Learning CNN Technique

6- Experiments and results Employ 1D-CNN. The NIDCNN model was created expressly to handle input that has only one dimension. Researchers have previously employed a number of general techniques as well as deep learning-based techniques for the identification of network intrusions. With 70% and 30% of the total data in each training set and testing set, respectively, we partitioned the dataset into two. Accuracy, precision, recall, and F-score were some of the metrics we used to evaluate the NIDCNN model's performance. The proposed system's findings are split into two groups based on the preprocessing methodology employed; the first group uses SVD to reduce features, and the second group does not utilize any feature reduction strategies.

6-1 Metrics and experimental setup:four metrics that are frequently employed for learning-based intrusion detection techniques are used to assess performance. TPR is used to assess how well the system performs in terms of identifying threats. FPR is employed to assess incorrect classifications of typical data. The harmonic mean of accuracy and TPR (recall) is the F-measure. Precision is defined as the ratio of true attacks to all other attacks. [19].

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

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F}_{measure} = 2\frac{* \text{ precision} * \text{recall}}{\text{precision} + \text{recall}}$$

Where:TP (true positive) refers to the number of attack data that is correctly identified as an attack,FP (false positive) refers to the number of normal data that is misidentified as an attack,FN (false negative) is the number of attack data that is mistakenly classified as normal,TN (true negative) is the number of normal data that is correctly classified as normal.

6.2 Result and Discuss: We demonstrate that, for the purpose of lowering the dimensionality of space, our suggested technique outperformed SVD. In order to accommodate input that has only one dimension, the NIDCNN model was created. For the purpose of identifying network breaches, researchers have previously used a variety of generic tactics as well as supplemental deep learning-based techniques. Practice accounts for 70% and training for 30% of the total data in these dataset divisions. In order to evaluate the performance of the NIDCNN model, we examined its accuracy, precision, recall, and F-score. Equations provide separate explanations for each metric.

A- Classification Model with SVD

The outcomes of applying SVD to minimize characteristics are described in this section in two different ways:

- **The NIDCNN Classification Model Using the SVD-10**

The results of the classification method's evaluation using the SVD-10 feature reduction approach are shown in Table 1. Figure (3) displays the data chart.

Table (1). Results of NIDCNN Classification Model With SVD-10.

Proposed type	Accuracy	Precision	Recall	F-score	Time in sec.
NIDCNNmodel with SVD-10	100%	100%	64%	78%	0.103

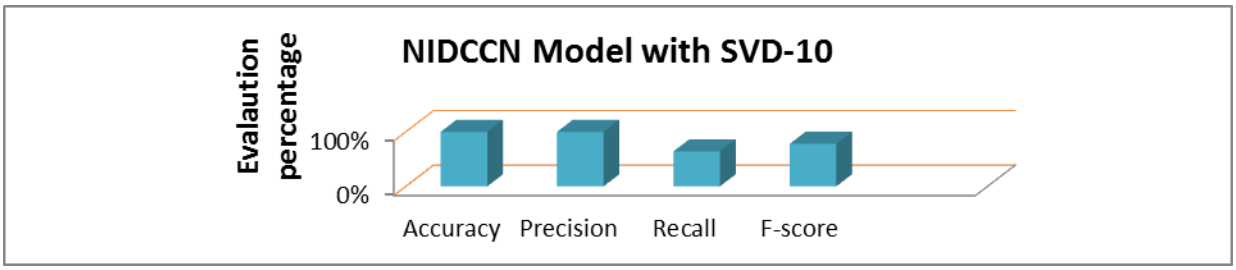

Fig. (3). Chart of NIDCNN Classification Model with SVD-10 Results.

•The NIDCNN Classification Model Using the SVD-15

The results of the classification method's evaluation using the SVD-15 feature reduction technique are shown in Table 2. In figure 4, the data chart is displayed.

Table (2). Results of NIDCNN Classification Model with SVD-15.

Proposed type	Accuracy	Precision	Recall	F-score	Time in sec.
NIDCNN model with SVD-15	100%	100%	64%	78%	0.27

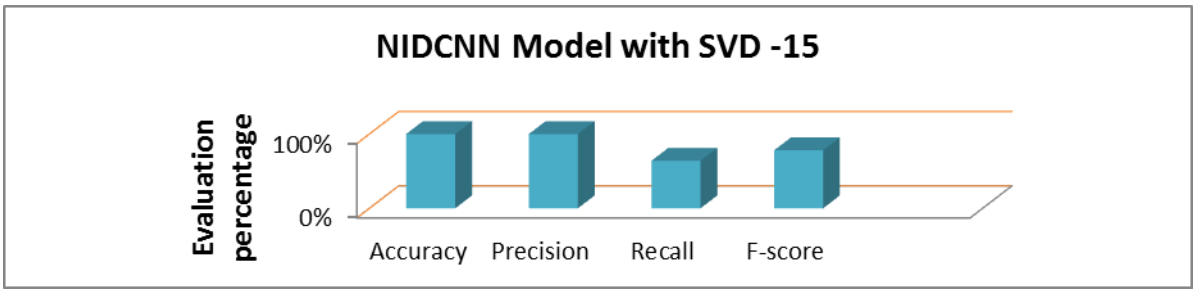

Fig. (4). Chart of NIDCNN Classification Model with SVD-15 Results

B- Classification Model without SVD

The suggested NIDCNN model for intrusion detection without the addition of feature reduction techniques is described in this section's results. These findings are presented in Table 4, and Figure 5 provides an explanation of the results chart.

Table (4) Results of NIDCNN Classification Model Without Feature Reduction.

Proposed type	Accuracy	Precision	Recall	F-score	Time in sec.
NIDCNN model without Feature Reduction	100%	100%	31%	48%	0.532

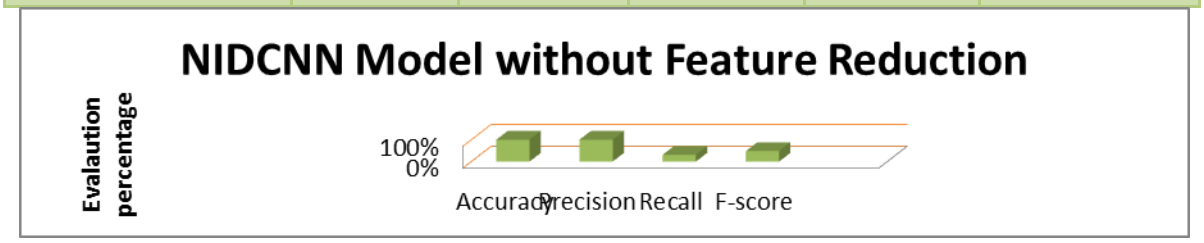

Fig. (5). Chart of NIDCNN Classification Model Without Feature Reduction Results.

Tables (1) to (4) show that we used the suggested 1D-CNN with SVD-15-based approaches to achieve 100% testing accuracy, 100% precision, 64% recall, and an F-score of 78%. The results are remarkably comparable, with a testing accuracy of 100%, a precision of 100%, a recall of 63%, and an F-score of 78% using 1D-CNN with SVD-10-based techniques. The results of the measurements were 100% accuracy, 100% precision, 31% recall, and 48% F-score when a NIDCNN was used instead. In order to make everything that was previously presented in the figures apparent and to show the efficiency of the suggested system without reduction strategies and its efficiency with the techniques present, Figure (6) carefully collected all the calculations given in Tables (1) through (4).

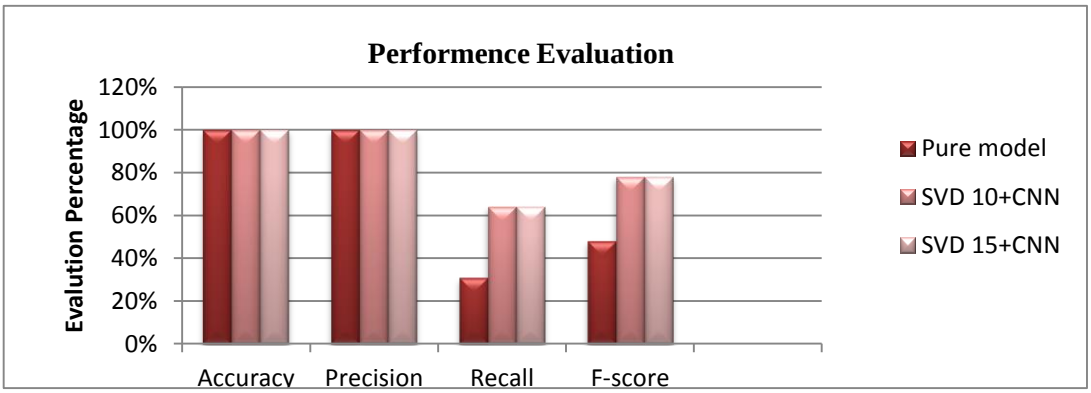

Fig. (6) The Performance Evaluation

Conclusion: proposed the NIDCNN system in this research. Our approach is innovative in that it uses deep learning-based detection techniques to improve cyber-threat detection. By comparing long-term security data, the suggested model system enables security analysts to respond to critical security alarms quickly and effectively. Having fewer false-positive alarms also makes it possible for security analysts to respond to cyber threats spread across numerous security events more quickly. Using a benchmark dataset (UN-SW-NB15), we demonstrated that our techniques may be used as one of the deep learning-based models for network intrusion detection by comparing them to an alternative method using well-known benchmark datasets. Second, by employing reduction techniques (SVD) to provide correct classifications, our solution fared better than traditional deep learning methods.

Further Work: In the future, to address the evolving problem of cyberattacks, we will focus on enhancing earlier threat predictions through multiple deep-learning approaches to discover the long-term patterns in the data. In addition, to improve the precision of datasets, the proposed NIDCNN model can be used to detect network intrusion in real-time, giving the opportunity to stop any potential intrusion problems and guaranteeing the security of user data.

References

[1] G. Wang et al., "A new approach to intrusion detection using artificial neural networks and fuzzy clustering", Expert Syst. Appl., vol. 37, pp. 6225–6232, 2010.

[2] M. Moradi and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks," Proc. of the 2004 IEEE International Conference on Advances in Intelligent Systems-Theory and Applications, pp. 148:1-6, Luxembourg, November 2004.

[3] Golub, G. H. and van Loan,C. F., "Matrix Computations", John Hopkins University Press, 3rd edition, 1996.

[4] Liao, Y. and Vemuri, V. R., Use of K-Nearest Neighbor Classifier for Intrusion Detection, Computers & Security, 21(5), (2002a), 439–448.

[5] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ''Deep learning approach for intelligent intrusion detection system,'' IEEE Access, vol. 7, pp. 41525–41550, 2019.

[6] M. Du, F. Li, G. Zheng, and V. Srikumar,‘‘DeepLog: Anomaly detection and diagnosis from system logs through deep learning,’’ in Proc. ACM CCS, Dallas, TX, USA, vol. 17, Nov. 2017, pp. 1285–1298.
[7]L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," Complex Adaptive Systems Conference Theme: Big Data, IoT, and AI for a Smarter Future Malvern, Pennsylvania, vol. 185, 239–247, June 16-18, 2021.
[8]G. Mahalakshmi et al.,"Intrusion Detection System Using Convolutional Neural Network on UNSW NB15 Dataset,"Advances in Parallel Computing Technologies and Applications, vol. 40, 1-8, 2021.
[9] S. Naseer,Y. Saleem,S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal,and K. Han, ‘‘Enhanced network anomaly detection based on deep neural networks,’’ IEEE Access, vol.6, pp. 48231–48246, 2018.
[10] W. Wang, Y. Sheng, and J. Wang, ‘‘HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,’’ IEEE Access, vol. 6, pp. 1792–1806, 2018.
[11] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ‘‘Deep learning approach for intelligent intrusion detection system,’’ IEEE Access, vol. 7, pp. 41525–41550, 2019.
[12]F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, ‘‘A novel twostage deep learning model for efficient network intrusion detection,’’ IEEE Access, vol. 7, pp. 30373–30385, 2019.
[13]Y. LeCun,Y. Bengio, and G. Hinton,‘‘Deep learning,’’ Nature, vol. 521, no. 7553, pp. 436–444, May 2015.
[14] A. Karpathy, ‘‘Connecting images and natural language,’’ Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 201
[15] Y. Shen, E. Mariconti, P. A.Vervier, and G. Stringhini, ‘‘Tiresias: Predicting security events through deep learning,’’ in Proc. ACM CCS, Toronto, ON, Canada, Oct. 2018, pp.592–605.
[16] D. Kalman,‘‘A singularly valuable decomposition: The SVD of a matrix,’’ College Math. J., vol. 27, no. 1, pp. 2–23, 1996.
[17] C. Khammassi and S. Krichen, ‘‘A GA-LR wrapper approach for feature selection in network intrusion detection,’’ Comput. Secur., vol. 70, pp. 255–277, Sep. 2017.
[18]N. Moustafa and J. Slay, ‘‘The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison

with the KDD99 data set,'' Inf. Secur. J., Global Perspective, vol. 25, nos. 1–3, pp. 18–31, 2016
[19]M. L. e. al., "Interpolation in Time Series: An Introductive Overview of Existing Methods, Their Performance Criteria and Uncertainty Assessment," *doi:10.3390/w9100796 www.mdpi.com/journal/water*, p. 796, 2017.

استخدام تحليل القيمة المفردة(SVD) لنظام كشف التسلل السريع القائم على التعلم العميق

انبثاق احمد شاكر[1]
قسم الحاسبات، كلية العلوم ،الجامعة المستنصرية بغداد، العراق
inbethaqahmed_2020@yahoo.com
7728509829
أ.د. احمد أبو الفتوح صالح[2]
قسم نظم المعلومات، كلية الحاسبات والمعلومات، جامعة المنصورة،المنصورة، مصر
elfetouh@mans.edu.eg
أ.د.حازم مختار البكري(3)
قسم نظم المعلومات، كلية الحاسبات والمعلومات، جامعة المنصورة، المنصورة، مصر
helbakry1@hotmail.com

مستخلص البحث:
تقنية الذكاء الاصطناعي القائمة على الشبكات العصبية الاصطناعية لتحديد المخاطر السيبرانية. اعتمدت مجموعة من المهن، بما في ذلك التعرف على أنماط أو فئات محددة، منهجيات التعلم العميق. تم استخدام البيانات من تقييمات كشف التسلل ومراقبة الأحداث الأمنية لتقييم حالة الشبكة. يجب تحسين أداء ودقة الكشف. قررنا اختبار مجموعة من الأساليب باستخدام مجموعة بيانات مفتوحة لتحديد أفضل نهج لاكتشاف التسلل. تهدف الدراسة الحالية إلى استكشاف إمكانية استخدام تحليل القيمة المفردة (SVD) كخطوة ما قبل المعالجة لتقليل أبعاد البيانات. بالإضافة إلى تقليل التشويش الناتج عن البيانات، تعمل خطوة المعالجة المسبقة هذه على تقليل أبعاد البيانات لتوفير الوقت في العمليات الحسابية. يمكن للاستراتيجية المقترحة أن تساعد الأساليب الأخرى المستخدمة حاليًا على الأداء بشكل أفضل. لقد قمنا باختبار استراتيجيات التخفيض على مجموعة بيانات UNSW-NB15، وكانت النتائج إيجابية للغاية.

الكلمات المفتاحية : كشف التسلل، تحليل القيمة المفردة(SVD) ، التعلم العميق، أمن الشبكات.
ملاحظة : هل البحث مستل من رسالة ماجستير او اطروحة دكتوراه ؟ نعم