Open Access Library Journal
2020, Volume 7, e6151
ISSN Online: 2333-9721
ISSN Print: 2333-9705

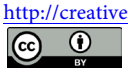
Recurrent Neural Networks & Deep Neural Networks Based on Intrusion Detection System

Rabeb Zarai[1*], Mnaouer Kachout[2,3], Mohamed A. G. Hazber[4], Mohammed A. Mahdi[4]

[1]College of Science, Gafsa University, Gafsa, Tunisia
[2]Department of Computer Engineering, College of Computer Science and Engineering, University of Hail, Hail, KSA
[3]Innov'Com, Sup'Com, Carthage University, Tunis, Tunisia
[4]Department of Computer Science and Information, College of Computer Science and Engineering, University of Hail, Hail, KSA
Email: *zarairabeb2@gmail.com

How to cite this paper: Zarai, R., Kachout, M., Hazber, M.A.G. and Mahdi, M.A. (2020) Recurrent Neural Networks & Deep Neural Networks Based on Intrusion Detection System. *Open Access Library Journal*, **7**: e6151.
https://doi.org/10.4236/oalib.1106151

Received: February 10, 2020
Accepted: March 22, 2020
Published: March 25, 2020



Abstract

The computer security has become a major challenge. Tools and mechanisms have been developed to ensure a level of compliance. These include the Intrusion Detection Systems (IDS). The principle of conventional IDS is to detect attempts to attack a network and to identify abnormal activities and behaviors. The reasons, including the uncertainty in searching for types of attacks and the increasing complexity of advanced cyber-attacks, IDS calls for the need for integration of methods such as Deep Neuron Networks (DNN) and Recurring Neuron Networks (RNN) more precisely long-term memory (LSTM). In this submission, DNN and LSTM were used to predict attacks against the Network Intrusion Detection System (NIDS). In this memory, we used four hidden layers for all deep learning algorithms, forty-one layers of inputs and two layers of outputs and with 100 iterations. In fact, learning is kept constant at 0.01 while the other parameters are optimized. After that for DNN, the number of neurons of the first hidden layer was further increased to 1280 but did not give any appreciable increase in accuracy. Therefore, the number of neurons has been set to 1024 and the LSTM we set the number of neurons of all hidden layers to 32. The results were compared and concluded that a three-layer LSTM performs better than all other conventional machine learning and deep learning algorithms.

Subject Areas

Computer Science & Communications, Engineering

Keywords

Intrusion Detection System (IDS), Deep Learning (DL),
Deep Neural Networks (DNN), Explainable Artificial Intelligence (AI),

Recurrent Neural Networks (RNN), Anomaly Detection

1. Introduction

Today, information systems represent the essential point of all enterprises, regardless of their size or sector of activity. Nevertheless, the data stored and the services rendered by these information systems present themselves as potential targets for various types of attacks. With their great diversity and specificity to systems, these attacks can have catastrophic consequences. In this context, computer security has become a major challenge, and work in this area of research is increasing. Various tools and mechanisms are developed to ensure a level of safety that meets the demands of modern life [1]. These tools include the Intrusion Detection System (IDS). IDS are tools designed to detect attempted attacks on a network, and to identify abnormal activities and behaviors that are designed to interfere with the proper functioning of the system. Intrusion detection is classified into network-based intrusion detection system (NIDS), host-based intrusion detection system (HIDS) and Hybrid IDS [2] [3] [4] [5] [6]. And detect malicious activity by monitoring the entire network traffic. IDS systems are installed in general by placing the network interface card in promiscuous mode to capture all networks traffic segments. While HIDS is used to monitor encrypted traffic data to a specific host. It works on information collected from within an individual computer system. Hybrid IDS bring together the characteristics of NIDS and HIDS. They allow, to monitor the network and terminals Network based IDS.

IDS are tools designed to detect unauthorized use, misuse and signature of the computer network by insiders or outsiders [7] [8] [9]. In order to detect attacks that a system may experience, it is necessary to have a specialized software to collect data passing through the system and which will be used subsequently in the detection process. There are several tools that can accomplish this task among them we cite network traffic sniffer like Wireshark, Snort, Prelude. However, the data from this collection tool are voluminous and their processing by existing methods is time-consuming.

Machine Learning (ML) based IDS systems based algorithms such as K-means, Hidden Markov Model and Self Organizing Maps (SOM) [10] [11] [12] [13]; Neural networks, decision trees, Naive Bayes and Support Vector Machine [9] [14] [15]. Not long ago, Deep learning (DL) has revolutionized a multitude of fields newly and has supplied state-of-the-art performances in fields such as computer vision and natural language processing [16] [17]. As a result of its deep structure, Deep Neural Networks (DNN) algorithms have the proficiency to learn complex patterns in data with multiple layers of abstraction [18], making them ideal candidates to learn complex patterns that located in network traffic data. As a result, DNN based IDS (DNN-IDS) algorithms have received expanded attention in recent work. The objective of this work is to propose a new approach based on learning algorithms that allow to prevent, detect and respond to an at-

tack in order not to allow the same aggression to recur. Detection allows the identification of a certain characteristic that violates security policies. Intrusion detectors (IDS) are used because of a lack of security in contemporary operating systems 5 or current programs. The large-scale deployment of IDS by anomalies is prevented by the too many false positives they generate. To reduce this number while improving detection accuracy, it is necessary to best adapt the IDS to the network it must monitor. Thus, we will propose a method to automate intrusion detection using deep learning algorithms that can provide an instant update of a new sample of malware by following its introduction into the classification.

The formatter will need to create these components, incorporating the applicable criteria that follow.

2. Approaches Deep Learning Based IDS

Deep learning is a subset of Machine learning. In practice, all deep learning algorithms are neural networks, which share some common basic properties. They are all made up of interconnected neurons arranged in layers. What differentiates them is the net-work architecture (or how neurons are organized in the network) and sometimes how they are formed.

This state of the art of IDS using deep learning techniques has allowed us to have a global view of what is being done today in this field. The choice of the model and its parameters will depend essentially on the desired outcome, in particular the fact that the IDS is a NIDS.

Behavioral IDS based on unsupervised machine learning techniques have a definite advantage since they do not need to know all the attacks to detect one. So they adapt to the evolution of the attacks.

In this spirit, we present the main methods of deep learning. The following list is not exhaustive, but it represents the vast majority of algorithms used today: Deep learning can be classified into two main classes according to the objectives for which it was designed: the deep networks of unsupervised learning and the deep networks of supervised learning.

2.1. Unsupervised Deep Learning Methods

Deep auto-encoders: The auto-encoder is an unsupervised learning algorithm based on artificial neural networks, which create a new representation of data sets. Recently, the concept of auto-encoder has become more widely used for generative model learning. The architecture of an auto-encoder consists of two parts such as the encoder and the decoder. F. Farahnakian *et al.* [19] proposed to use Deep Auto-Encoder (DAE) as one of the most well-known deep learning models. The proposed DAE model is formed in an avid layer way to avoid overflow and local optimum. The experimental results of the KDD-CUP 99 dataset show that our approach makes for substantial improvements over other approaches based on in-depth learning in precision, detection rates and false alarm rates.

Restricted Boltzmann Machines: Restricted Boltzmann Machines or RBM is a type of artificial neural networks, where neurons are organized into two layers, namely visible and masked. Unlike direct retransmission networks, RBM data can flow in both directions from visible units to hidden units, and vice versa. RBM is one of the most popular in-depth learning tools because of its ability to know the distribution of the probability of entry in a supervised and unsupervised manner. It was introduced by Paul Smolensky in 1986 with the name Harmonium. S. Seo *et al.* [20] defined RBM as a type of unsupervised learning that does not use class labels. RBM is a probabilistic generative model that composes new input data data based on formed probability. The new data compiled by RBM shows that noise and outliers are removed from the input data. When newly composed data is applied to the network intrusion detection model, the negative effects of noise and outliers on learning are eliminated. They offer noise and outlier values in KDD Cup99 Data are removed by applying the data to RBM and composing a new data. Then use the results between the existing data and the data from which the noises and outliers are removed.

2.2. Supervised Deep Learning Methods

Recurrent Neural Networks: A Recurrent Neural Networks or RNN looks like a traditional neural network are artificial neural networks. In a traditional neural network, the model produces the output by multiplying the input with the weight and activation function. In the RNN, information can spread in both directions, including from deep layers to the first layers. In this, they are closer to the true functioning of the nervous system, which is not one-way. These networks have recurring connections in the sense that they keep information in memory. In theory, RNN is supposed to transport information on time. However, it is quite difficult to spread all this information when the time step is too long. When a network has too many deep layers, it becomes unmanageable. This problem is called: Disappearance gradient problem. If you remember, the neural network updates the weight using the gradient descent algorithm. Gradients decrease when the network descends to the lower layers. To overcome the potential disappearance gradient problem encountered by RNN, three researchers, Hochreiter, Schmidhuber and Bengio improved the RNN with an architecture called Short-term Memory (LSTM). R. Vinayakumar *et al.* [21] this article describes how sequential data modelling is a relevant cyber security task. In addition, stacked recurring neural networks (S-RNN) have the potential to quickly learn complex temporal behaviors, including sparse representations. To do this, the authors model network traffic as a time series, especially transmission control protocol/internet protocol (TCP/IP) packets in a predefined time range with a supervised learning method, using millions of known good and bad network connections. To discover the best architecture, the authors complete a comprehensive review of various RNN architectures with its network parameters and network structures. They use the login records of the Kddcup-99 challenge dataset.

Artificial Neural Networks: Artificial neural networks or ANN are inspired by the human brain and are composed of interconnected artificial neurons capable of certain calculations on their inputs. The input data activates the neurons in the first layer of the network whose output is the input into the second layer of neurons in the network. Similarly, each layer passes to the next layer and the last layer produces the result. When an ANN is used as a classifier, the output layer generates the final classification category. V. Golovko *et al.* [22] proposed to use artificial immune systems and neural networks to detect attacks on computer systems. The principles of the design of the attack detection system based on the artificial immune network are described, and the architecture of the attack detection system is presented.

Deep Neural Networks: A Deep Neural Networks or DNN are artificial neural networks (ANN) with a multilayer structure within the input-output layers. They can model complex non-linear relationships and can generate computational models where the object is expressed in terms of stratified composition of primitives. Deep Neural Networks has revolutionized a multitude of fields in recent years and has provided cutting-edge performance in areas such as computer vision and natural language processing. Kasun *et al.* [23] proposed a methodology to generate offline and online feedback to the user on the DNN-IDS decision-making process. Offline, the user is reported the input features that are most relevant to detect each type of intrusion by the trained DNN-IDS. Online, for each detection, the user is reported the input features that contributed the most to the detection. This can be binomial where the data indicates the presence or absence of an attack, where it can be multinomial where the input record can be from a specific attack group.

3. Proposed Approaches

We have proposed three approaches to Intrusion Detection System based on deep learning algorithms (DNN and RNN) with a Kddcup99 database that define us in the next chapter.

3.1. DNN Based Intrusion Detection System

We proposed an algorithm of deep neural networks or DNN that contains 41 layers of input, 4 layers of hidden and 2 layers of output, the neurons in input-layer to hidden-layer and hidden to output-layer are connected completely, and with 100 iterations. Indeed, the learning is kept constant at 0.01 while the other parameters are optimized. After that for DNN, the number of neurons of the first hidden layer was further increased to 1280 but did not give any appreciable increase in accuracy. Therefore, the number of neurons was set to 1024. We preferred Relu activations for hidden layers (for reasons that the Relu activation function is the most used in neural network architectures and more particularly in convolutional networks, where it has proven to be more effective than the widely used logistics sigmoid function. Since 2017, this activation function is the most popular for deep neural networks) and softmax for the output layers to other activation functions.

Conventionally, increasing the count of the layers results in better results compared to increasing the neuron count in a layer. Therefore, the following network topologies were used in order to scrutinize and conclude the optimum network structure for our input data. We proposed a DNN architecture with 1, 2, 3, 4 layers for all use cases, as shown in Figure 1. The detailed information and configuration details of the DNN architecture is shown in Figure 2.

3.2. RNN Based Intrusion Detection System

Considering that recurring neural networks (RNN) with short-term memory (LSTM) can learn from feature representations and automatically model long-term temporal dependencies, as we have seen in Part 7, we offer a fully connected deep LSTM end-to-end for attack-based action recognition. We set the number of neurons of all hidden layers to 8 then 16 and finally 32.

We proposed a RNN architecture as shown in Figure 3. The detailed information and configuration details of the RNN architecture is shown in Figure 4.

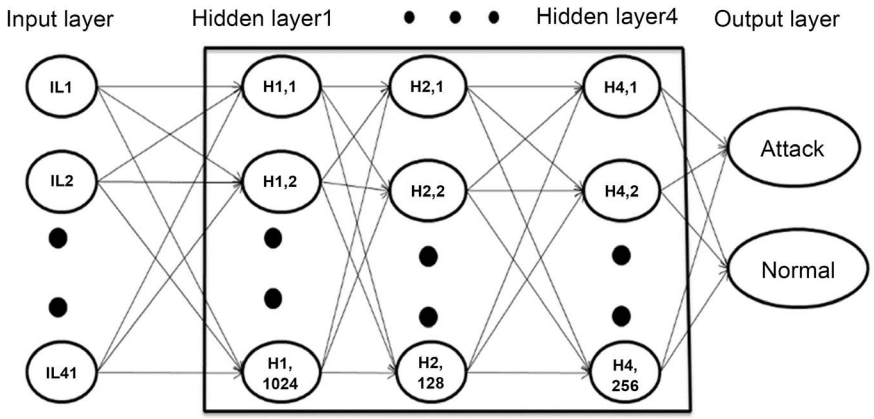


Figure 1. Proposed architecture of DNN.

Layer (type)	Output Shape	Param #
dense_1 (Dense)	(None, 1024)	43008
dropout_1 (Dropout)	(None, 1024)	0
dense_2 (Dense)	(None, 768)	787200
dropout_2 (Dropout)	(None, 768)	0
dense_3 (Dense)	(None, 512)	393728
dropout_3 (Dropout)	(None, 512)	0
dense_4 (Dense)	(None, 256)	131328
dropout_4 (Dropout)	(None, 256)	0
dense_5 (Dense)	(None, 1)	257
activation_1 (Activation)	(None, 1)	0

Figure 2. Capture of configuration of the proposed DNN model.

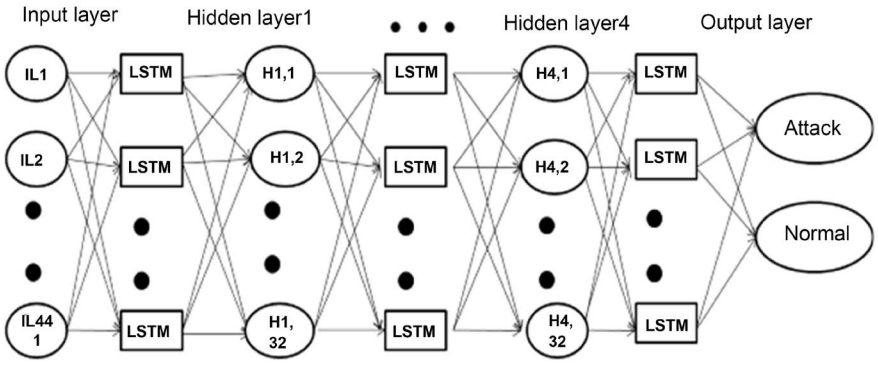


Figure 3. Proposed architecture of RNN.

Layer (type)	Output Shape	Param #
lstm_1 (LSTM)	(None, None, 32)	9472
dropout_1 (Dropout)	(None, None, 32)	0
lstm_2 (LSTM)	(None, None, 32)	8320
dropout_2 (Dropout)	(None, None, 32)	0
lstm_3 (LSTM)	(None, None, 32)	8320
dropout_3 (Dropout)	(None, None, 32)	0
lstm_4 (LSTM)	(None, 32)	8320
dropout_4 (Dropout)	(None, 32)	0
dense_1 (Dense)	(None, 1)	33
activation_1 (Activation)	(None, 1)	0

Figure 4. Capture of configuration of the proposed RNN model.

3.3. DATASET Used in NIDS

For several years, research groups have created datasets for Sdis. These collections provide learning data and tests for the various deep learning models. In addition, they offer the possibility to compare the performance of several IDS on the same data collection. These datasets represent system information grouped together. These data are obtained either by simulators or by real systems

The data used for our experiments are actual data from the KDD-Cup 99 database. These data are constructed from data collected and controlled by MIT Lindcoln laboratories for the DARPA 1998 intrusion detection evaluation program. This is the data set used in the third international competition on Knowledge Exploration and Data Mining tools, which was held in conjunction with KDD-99, the fifth international conference on knowledge discovery and data mining. The task of the competition was to build a network intrusion detector, a predictive model able to distinguish between “bad” connections, called intrusions or attacks.

The dataset contains 41 features and 5 classes ("Normal", "DoS", "Probe", "R2L", "U2R").

- DOS (Deni of service): a denial-of-service attack is a type of attack in which the hacker generates computing or memory resources that are too busy or too saturated to meet legitimate network demands, thus preventing users from accessing memory resources.
- Probe: its actions are not really attacks since they are not destructive, they do not prevent an entity from functioning properly, but allow to acquire information sometimes crucial to conduct a larger attack later.
- U2R (User to Root attacks): a remote user attack is an attack in which a user sends packets to a machine via the Internet, which it does not have access to in case exposing the vulnerabilities of the machine and exploiting the privileges that a local user would have on the machine.
- R2L (Remote to Local access): its attacks are operations in which the hacker starts on the system with a normal user account and tries to abuse system vulnerabilities in order to obtain super user rights.

Table 1 gives the exact distribution of a sample of 10% of the data used during the competition different connection labels.

4. Results

In order to assess our approach to detecting anomalies, we compared the four commonly used defect detection model architectures is shown in Table 2 and concluded that DNN3 is more effective.

With respect to the evaluation of the LSTM anomaly detection model, we compared the four commonly used anomaly detection model architectures is shown in Table 3 and concluded that LSTM3 is more effective.

In order to assess the performance of our proposed approaches for detecting anomalies, we compared with other commonly used models for detecting anomalies and concluded that our approaches are fast is shown in Table 4.

To conclude on the results obtained, we can say that this approach based on deep two-layer learning algorithms makes it possible to prevent, detect and respond to an attack in order not to allow the same aggression to recur. Detection allows the identification of a certain characteristic that violates security policies. This method allowed us to automate intrusion detection using Deep Learning (Machine Learning) algorithms allowed us to provide an instant update of a new malware sample following its introduction into the classification system. As already mentioned, our findings are interesting. However, there are still areas for improvement in this approach.

Table 1. Description of 10% KDDcup99 data set.

	Type of attack					
KDD-Cup 99	Normal	DOS	Probe	R2L	U2R	Total
10% for Train	97,278	391,458	4107	1126	52	494,021
10% for test	60,593	229,853	4166	16,189	228	311,029

Table 2. Evaluation of the proposed approach for DNN.

Algorithm	Accuracy	Precision	Rappel	F1-score
DNN1	0.929	0.998	0.915	0.954
DNN2	0.929	0.998	0.914	0.954
DNN3	0.930	0.997	0.915	0.955
DNN4	0.929	0.999	0.913	0.954

Table 3. Evaluation of the proposed approach for LSTM.

Algorithm	Accuracy	Precision	Rappel	F1-score
LSTM1	0.929	0.996	0.909	0.950
LSTM2	0.938	0.999	0.923	0.960
LSTM3	0.983	0.999	0.979	0.998

Table 4. Evaluating our proposed approaches with other existing approaches.

Algorithm	Accuracy	Precision	Rappel	F1-score
Our approach LSTM	**0.983**	**1.00**	**0.979**	**0.998**
Our approach DNN	**0.930**	**0.997**	**0.915**	**0.955**
Navie Bayes	0.929	0.988	0.923	0.955
DecisionTree	0.928	0.999	0.912	0.953
SVM	0.841	0.607	0.774	0.680

5. Conclusions

The objective of this work was to propose a new approach based on learning algorithms that makes it possible to prevent, detect and respond to an attack in order not to allow the same aggression to recur. Detection allows the identification of a certain characteristic that violates security policies. This allowed us to automate intrusion detection using deep learning (Deep Learning) algorithms, which provided an instant update of a new malware sample following its introduction into the classification system. The results are interesting. However, there are still areas for improvement in this approach.

The future of network security technologies may be in the further integration of the various available deep learning tools to ensure network security, because the administration of equipment safety is an increasingly complex and extensive task, while security needs are growing. The usefulness of DNN and LSTM in the SDI has been presented in detail in this chapter. Other conventional ML algorithms and other DL algorithms were taken into account, the Kdd-Cup 99 dataset was mainly used as a benchmarking tool for the study, thanks to which the superiority of the DNN and LSTM on the other compared algorithms was clearly documented. To further refine the algorithm, this document takes into account LSTM with different numbers of hidden layers and it was concluded that a three-layer LSTM was effective and accurate for all.

The future of network security technologies may be in the further integration of the various available tools of deep learning (Convolutional Neural Networks or CNN) to ensure the security of a network.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Park, Y.S., Choi, C.S., Jang, C., Shin, D.G., Cho, G.C. and Kim, H.S. (2019) Development of Incident Response Tool for Cyber Security Training Based on Virtualization and Cloud. 2019 *International Workshop on Big Data and Information Security* (*IWBIS*), Bali, Indonesia, 115-118. https://doi.org/10.1109/IWBIS.2019.8935723

[2] Alom, M.Z. and Taha, T.M. (2017) Network Intrusion Detection for Cyber Security Using Unsupervised Deep Learning Approaches. 2017 *IEEE National Aerospace and Electronics Conference* (*NAECON*), Dayton, OH, 63-69. https://doi.org/10.1109/NAECON.2017.8268746

[3] Mehra, L., Gupta, M.K. and Gill, H.S. (2015) An Effectual & Secure Approach for the Detection and Efficient Searching of Network Intrusion Detection System (NIDS). 2015 *International Conference on Computer*, *Communication and Control*, Indore, 21-23 April 2015, 1-5. https://doi.org/10.1109/IC4.2015.7375615

[4] Manthira, M.S. and Rajeswari, M. (2013) Virtual Host Based Intrusion Detection System for Cloud. *International Journal of Engineering and Technology*, **5**, 5023-5029.

[5] Torkaman, A., Javadzadeh, G. and Bahrololum, M. (2013) A Hybrid Intelligent HIDS Model Using Two-Layer Genetic Algorithm and Neural Network. *The* 5*th Conference on Information and Knowledge Technology*, Shiraz, 28-30 May 2013, 92-96. https://doi.org/10.1109/IKT.2013.6620045

[6] Shidore, S. and Bhusari, V.K. (2014) Evasion of Network Intrusion Detection System Using Functional Framework. *International Journal of Application or Innovation in Engineering & Management*, **3**.

[7] Ahmed, P., Mona, T., Kaveh, B. and Joaquim. (2012) An Intrusion Detection And Prevention System in Cloud Computing: A Systematic Review. *Journal of Network and Computer Applications*, **36**.

[8] Kumari, U. and Soni, U. (2017) A Review of Intrusion Detection Using Anomaly Based Detection. 2017 2*nd International Conference on Communication and Electronics Systems* (*ICCES*), Coimbatore, 19-20 October 2017, 824-826. https://doi.org/10.1109/CESYS.2017.8321199

[9] Justin, V., Marathe, N. and Dongre, N. (2017) Hybrid IDS Using SVM Classifier for Detecting DoS Attack in MANET Application. 2017 *International Conference on I-SMAC* (*IoT in Social*, *Mobile*, *Analytics and Cloud*), Palladam, 10-11 February 2017, 775-778. https://doi.org/10.1109/I-SMAC.2017.8058284

[10] Mishra, P., Varadharajan, V., Tupakula, U. and Pilli, E.S. (2019) A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection. *IEEE Communications Surveys & Tutorials*, **21**, 686-728. https://doi.org/10.1109/COMST.2018.2847722

[11] Xiong, C., Hua, Z., Lv, K. and Li, X. (2016) An Improved K-Means Text Clustering Algorithm by Optimizing Initial Cluster Centers. 2016 7*th International Conference on Cloud Computing and Big Data* (*CCBD*), Macau, 16-18 November 2016, 265-268. https://doi.org/10.1109/CCBD.2016.059

[12] Yongzhong, L., Rushan, W., Jing, X., Ge, Y. and Bo, Z. (2009) Intrusion Detection Method Based on Fuzzy Hidden Markov Model. 2009 6*th International Conference on Fuzzy Systems and Knowledge Discovery*, Tianjin, 14-16 August 2009, 470-474.

https://doi.org/10.1109/FSKD.2009.79

[13] Wang, H., Xu, Z., Wang, C. and Yuan, Z. (2009) A New Algorithm Combining Self Organizing Map with Simulated Annealing Used in Intrusion Detection. 2009 2*nd International Conference on Biomedical Engineering and Informatics*, Tianjin, 17-19 October 2009, 1-4. https://doi.org/10.1109/BMEI.2009.5305521

[14] Wei, M., Liu, Y., Chen, X. and Li, J. (2010) Decision Tree Applied in Web-Based Intrusion Detection System. 2010 2*nd International Conference on Future Networks*, Sanya, Hainan, 22-24 January 2010, 110-113. https://doi.org/10.1109/ICFN.2010.68

[15] Ernawati, S., Yulia, E.R. and Samudi, F. (2018) Implementation of The Naïve Bayes Algorithm with Feature Selection Using Genetic Algorithm for Sentiment Review Analysis of Fashion Online Companies. 2018 6*th International Conference on Cyber and IT Service Management* (*CITSM*), Parapat, Indonesia, 7-9 August 2018, 1-5. https://doi.org/10.1109/CITSM.2018.8674286

[16] Wang, S. and Jiang, J. (2016) Learning Natural Language Inference with LST. *Proceedings of NAACL-HLT* 2016, San Diego, CA, 12-17 June 2016, 1442–1451.

[17] Muhammed, M.A.E., Ahmed, A.A. and Khalid, T.A. (2017) Benchmark Analysis of Popular ImageNet Classification Deep CNN Architectures. 2017 *International Conference On Smart Technologies for Smart Nation* (*SmartTechCon*), Bangalore, 17-19 August 2017, 902-907. https://doi.org/10.1109/SmartTechCon.2017.8358502

[18] LeCun, Y., *et al.* (2015) Deep Learning. *Nature*, **521**, 436-444. https://doi.org/10.1038/nature14539

[19] Farahnakian, F. and Heikkonen, J. (2018) A Deep Auto-Encoder Based Approach for Intrusion Detection System. 2018 20*th International Conference on Advanced Communication Technology* (*ICACT*), Chuncheon-Si Gangwon-Do, Korea (South), 11-14 February 2018, 247-252. https://doi.org/10.23919/ICACT.2018.8323688

[20] Seo, S., Park, S. and Kim, J. (2016) Improvement of Network Intrusion Detection Accuracy by Using Restricted Boltzmann Machine. 2016 8*th International Conference on Computational Intelligence and Communication Networks* (*CICN*), Tehri, 23-25 December 2016, 413-417. https://doi.org/10.1109/CICN.2016.87

[21] Vinayakumar, R., Soman, K. and Prabaharan, P. (2020) Evaluation of Recurrent Neural Network and Its Variants for Intrusion Detection System (IDS). https://doi.org/10.4018/978-1-7998-0414-7.ch018

[22] Golovko, V., Komar, M. and Sachenko, A. (2010) Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers. 2010 *International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET*), Lviv-Slavske, 237-237.

[23] Amarasinghe, K. and Manic, M. (2018) Improving User Trust on Deep Neural Networks Based Intrusion Detection Systems. *IECON* 2018-44*th Annual Conference of the IEEE Industrial Electronics Society*, Washington DC, 21-23 October 2018, 3262-3268. https://doi.org/10.1109/IECON.2018.8591322