Intrusion Detection System Using Deep Belief Network With Grass Hopper Optimization Approach (DBNGOA-IDS)

Dr. S. Rajeshwari*
*Assistant Professor, Department of Computer Science, Hindusthan College of Arts & Science, TamilNadu, India.

Abstract - Information security is greatly aided by intrusion detection, and the essential technology is the ability to precisely identify different network threats. This research explores deep learning models for intrusion detection systems and proposes a deep learning strategy for intrusion detection utilizing Deep belief network and grasshopper (DBNGOA-IDS). Additionally, the model's performance is investigated in binary classification and multiclass classification, as well as how the number of neurons and various learning rates affect the performance of the suggested model. The performance of the present study is compared with other machine learning techniques on the benchmark data set.The experimental results demonstrate that DBNGOA-IDS performs better than typical machine learning classification methods in both binary and multiclass classification, and that it is particularly well suited for modeling a classification model with high accuracy.The DBNGOA-IDS model enhances intrusion detection accuracy and offers an innovative method to intrusion detection.

Keywords: Information security, machine learning, Intrusion detection, deep learning.

1. Introduction

A wide range of security threats attacks target computer networks including wireless networks in particular. The wireless communication medium's openness, adaptability, and mobility present security concerns that must be overcome [1], [2]. A crucial technical problem that cannot be avoided is how to recognize different network attacks, particularly unanticipated ones.An incursion can be detected using an intrusion detection system (IDS), a key research advancement in the field of information security. An intrusion can be either ongoing or have already happened. In reality, intrusion detection is typically equivalent to a classification problem, such as a binary, multiclass, or five-category classification problem, which determines whether network traffic behavior is normal or any of the other attack types.

In other words, the primary goal of intrusion detection is to increase the effectiveness of classifiers in correctly identifying the invasive behavior. Machine learning approaches have been widely utilized to recognize different sorts of assaults, and a machine learning strategy can assist the network administrator in taking the necessary precautions to stop invasions. However, the majority of existing machine learning techniques are based on shallow learning, and research frequently place an emphasis on feature engineering and selection. As a result, research is unable to address the issue of huge intrusion data categorization that occurs in a real-world network application environment [3].

Multiple classifications will result in lower accuracy due to the dynamic expansion of data sets. Shallow learning is also inadequate to high-dimensional learning with vast amounts of data, which is required for predicting and intelligent analysis. Deep learners, on the other hand, have the ability to draw better representations from the data and build far better models.

Due to the recent extremely quick growth of deep learning theory and technology, a new era of artificial intelligence has begun, providing a completely new method for creating intelligent intrusion detection technologies.

Deep belief network (DBN), which have been around for decades but whose full potential has only recently started to become widely recognized, similar to convolutional neural networks (CNNs), have recently generated a significant development in the field of deep learning due to growing computational resources [4]. DBN have been utilized extensively in a variety of disciplines recently, including computer vision, natural language processing (NLP), semantic comprehension, speech recognition, language modeling, translation, image description, and human action recognition [5]–[8].

Through studies, Zhang [9] discovered the key factors that should be used to set the hidden layer node count, learning rate, and number of iterations' effects on the DBN's capacity for feature extraction. However, network settings are still changed based on experience when choosing parameters for DBN. This research developed a new IDS method based on DBN to provide a set of ideal detection schemes. To lessen the impact of manual parameter setting on training results, parameter optimization is first carried out using GOA. Next, the impact of the best network structure distribution and parameter optimization on the hidden layer's capacity to extract features is examined. The preprocessed data is then used to train the network, and a DBN-based intrusion detection model is developed.

- A deep learning strategy for an intrusion detection system is proposed by employing deep neural network (DBNGOA-IDS) because deep learning has the potential to extract better representations from the data to construct significantly better models.
- Demonstrate the conception and application of the DBNGOA-based detection system. Additionally, the model's performance is investigatedin binary classification and multiclass classification, as well as the effects of different learning rates and the number of neurons on accuracy.

- On the benchmark NSL-KDD dataset, research examines how well the traditional machine learning approaches perform in multiclass classification.

Compared the performance proposed DBNGOA-IDS with various machine learning techniques. The experimental findings show that DBNGOA-IDS are ideally suited for intrusion detection. The performance of DBNGOA-IDS is superior to the conventional classification approach on the NSL-KDD dataset in both binary and multiclass classification, and it increases the accuracy of intrusion detection.

2. Related works

Studies have demonstrated that deep learning completely surpasses traditional techniques, making it a prominent subset of machine learning that has been employed for intrusion detection. In this section prior study on DBN based intrusion detection is discussed.

Ying Zhang et al [10] provide an enhanced genetic algorithm (GA) and deep belief network (DBN)-based intrusion detection model. In order for the intrusion detection model based on the DBN to attain a high detection rate with a small structure, facing various forms of attacks, the optimal number of hidden layers and number of neurons in each layer are created adaptively by numerous iterations of the GA. Finally, the model and methods were simulated and evaluated using the NSL-KDD dataset. The experimental findings demonstrate that combining the improved intrusion detection model with DBN can significantly increase the rate at which intrusion threats are recognized while lowering the complexity of the neural network's structure.

To improve the network structure of the DBN, Peng Wei [11] suggests a novel joint optimization approach. First, a particle swarm optimization (PSO) based on the learning factor and adaptive inertia weight is developed. Then optimize the PSO to discover the first optimization solution using the fish swarm behavior of cluster, foraging, and other behaviors. The genetic operators with self-adjusting crossover probability and mutation probability are then used to optimize the PSO in order to search for the overall optimization solution based on the original optimization solution. The network topology of the intrusion detection classification model is then created using the global optimization solution created by the aforementioned joint optimization method. This DBN - IDS improves the average classification accuracy by at least 1.3% and up to 14.80% in the five-category classification, which is proved to be an efficient DBN-IDS optimization method.

Othmane Belarbi et al [12] develop and assess Deep Belief Networks' (DBNs') capabilities for detecting cyber attacks across a network of connected devices. The CICIDS2017 dataset was utilized to train the DBN technique and evaluate its effectiveness. Numerous class balance strategies were used and assessed. Finally, contrast they strategy with both the current state-of-the-art and a traditional Multi-Layer Perceptron (MLP) model. The findings of they suggested DBN technique are competitive and encouraging, with a notable boost in performance for the identification of attacks that are underrepresented in the training dataset.

Deep Belief Network and Particle Swarm Optimization are used by Sajith et al. [13] to classify intrusions into groups like Normal, Probe, DoS, U2R, and R2L. DARPA 1999 is the dataset used to test this model, and it is evaluated using a variety of metrics. The suggested method also performs better when compared to existing systems like ANFIS, HHO, and Fuzzy GNP, with an accuracy of 96.5%.

A smart strategy or technique to defend the security breach is presented by Nagaraj Balakrishnanet al [14] developed with the improvement of Deep Learning algorithms i.e., Deep Belief Network. The hostile activity that is active within the network is examined by this intelligent intrusion detection technology, and attempts are made to gain access. The examination of embedding the Deep Learning methodology is covered in this work. The security network's DBN enhancement is contrasted with traditional DGAs and IDS algorithms, and the outcomes are examined.

3. Proposed Methodology

The present IDS includes Deep belief network with grasshopper optimization. GOA is used to identify both the ideal parameter combination and the ideal network structure simultaneously. The network structure whose RMSE converges to the lowest value is thought to be the best after looking for the ideal parameter combination for the network with various topologies under the same training conditions.First, GOA searches the [0, 1] and [1, 100], respectively, search ranges for the best learning rate and batch extraction parameters in DBN.First, using search ranges of [0, 1] and [1, 100], respectively, GOA searches for the best learning rate and batch extraction parameters in DBN. The parameter search for various network structures begins when the optimization algorithm's parameters have been specified. The iteration starts to converge, showing that the method has significant global optimization capabilities and a quick convergence rate, making it suited for finding the best DBN parameter combinations. The DBN model also has a positive training impact and tends to stabilize after 100 iterations. The proposed DBNGOA working procedure is shown in figure 1.

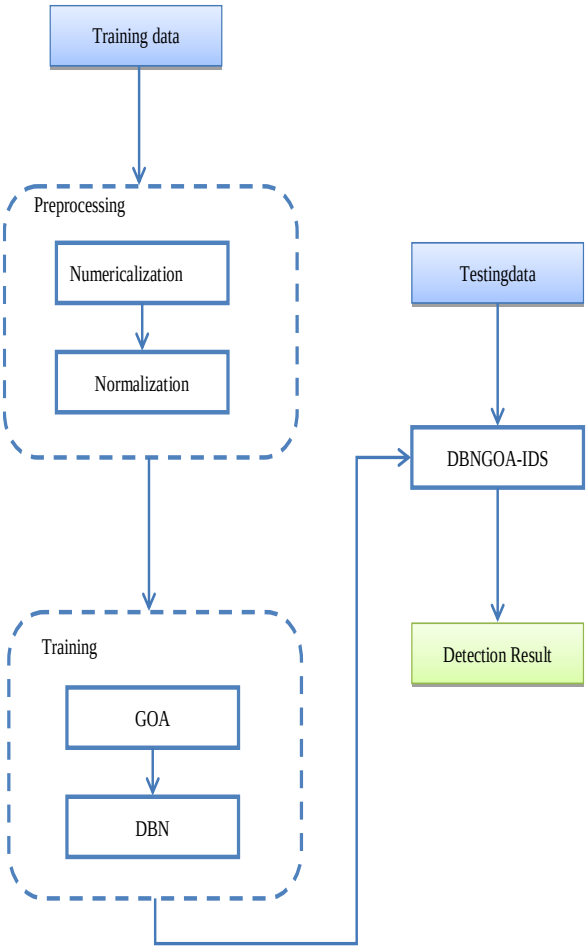

Figure 1. Proposed DBNGOA- IDS framework

3.1 Dataset Description

Numerous intrusion detection experiments make use of the 2009 NSL-KDD dataset. The NSL-KDD dataset is used as the benchmark dataset by all researchers in the most recent literature[15-17] because it not only resolves the inherent redundant records issues of the KDD Cup 1999 dataset but also keeps the number of records in the training set and testing set reasonable, preventing the classifier from favoring more frequent records.

	Total instance	Normal	Dos	Probe	R2L	U2R
KDDTrain+	125973	67343	45927	11656	995	52
KDDTest+	22544	9711	7458	2421	2754	200
KDDTest21	11850	2152	4342	2402	2754	200

As indicated in Table 1, the dataset includes the KDD Train+ dataset as the training set, as well as the KDD Test + and KDDTest21 datasets as the testing set. These datasets contain various normal records and four different types of attack records. A subset of the KDD Test+ dataset that is more challenging to classify is the KDDTest-21 dataset.
Every traffic record has one class label and 41 features, which comprise basic features, content features, and traffic features. Attacks in the dataset are divided into four groups based on their characteristics: DoS (Denial of Service), R2L (Root to Local), U2R (User to Root), and Probe (Probing Attacks). It is possible to give a more realistic theoretical foundation for intrusion detection by using the testing set, which contains some unique attack types that vanish in the training set.

3.2 DATA PREPROCESSING

NUMERICALIZATION

The NSL-KDD dataset consists of 3 nonnumeric characteristics and 38 numeric features. Research must convert several nonnumeric features, including "protocol_type," "service," and "flag" features, into numeric form because the input value of DBNGOA-IDS -IDS should be a numeric matrix.

NORMALIZATION

First, according to some features, the difference between the maximum and minimum values has a very large scope, so the logarithmic scaling method is applied for scaling to obtain the average ranges. Second, the value of every feature is mapped to the [0, 1] range linearly according to (1), where Max denotes the maximum value and Min denotes minimum value for each feature.

$$d_a = \frac{d_a - m_x}{m_n} \quad (1)$$

3.3 METHODS

Deep Belief Network

One of the most popular deep learning algorithms is the deep belief network (DBN), which was first proposed by Hinton [18]. This algorithm learns quickly and can locate the ideal settings more quickly than the others [19]. A restricted Boltzmann machine (RBM)-based unsupervised learning module and a logistic regression layer are the key components of a traditional DBN [20].

The Restricted Boltzmann Machine (RBM) is a widely used stochastic neural network that builds a deep belief network (DBN) using layer-wise training. A layer of Boolean hidden neurons and a layer of binary-valued neurons are both present in the RBM. Although there are symmetrical and bidirectional connections between the layers, there are none between the neurons in the same layer.

The learning process of a layer-wise configuration is based on the energy function of the configuration, which is defined in (2), to learn a probability distribution between the two levels. As a result, the following equation expresses the probability distribution.

$$Ef(a,b) = -\sum_{m=1}^{z_a} x_m a_m - \sum_{n=1}^{z_b} y_n b_n - \sum_{m=1}^{z_a}\sum_{n=1}^{z_b} b_n W_{n,m} \quad (2)$$

$$pd = \frac{e^{-Ef(a,b)}}{\sum_a \sum_b e^{-Ef(a,b)}} \quad (3)$$

The number of neurons in the visible layer is b_m, the number of Boolean hidden neurons in the hidden layer is b_n, the weight matrices between the visible layer and the hidden layer are $W_{n,m}$, and the biases for the t layers are x_m and y_n.

Next, an equation containing the activation probability functions is shown.

$$pd(a_m = 1|b) = sig\left(\alpha_m + \sum_{n=1}^{i_b} W_{n,m} b_m\right) \quad (4)$$

$$pd(b_m = 1|a) = sig\left(y_m + \sum_{m=1}^{i_a} W_{n,m} a_n\right) \quad (5)$$

And the logistic sigmoid function is represented by sig (). As a result, the pre-training principles allow for the unsupervised technique of training the weight matrices and layer biases.The data's features cannot be captured by a single hidden restricted Boltzmann machine (RBM). Progressively extracting deep features from the input dataset is possible with a deep belief network (DBN), which is built by stacking layers of restricted Boltzmann machines (RMBs) in a hierarchical manner and finishing with a logistic regression layer.Using the training data as inputs, the first RBM of the DBN is pre-trained as an independent RBM. When the weight matrix and bias parameters of the first RBM are established, the output from the first RBM is then chosen as the input to the second RBM. Next, the initial two RBMs' hidden layers can be thought of as a new RBM and are iteratively trained using the same process.The final step involves stacking a common predictor (such a layer for logistic regression) on top of the entire network and training it under supervision. The back-propagation (BP) technique is used for fine tuning to slightly alter the parameters of the entire trained network once the aforementioned steps have been applied.

GRASSHOPPER OPTIMIZATION ALGORITHM

The GOA algorithm, a recent and intriguing swarm intelligence system that imitates grasshoppers' natural foraging and swarming behaviors, was put forth by Saremi et al. in [21]. Grasshoppers are insects that are well-known for being harmful pests that interfere with and harm agricultural and crop productivity [21], [22]. Nymph and maturity are two stages in their life cycle. While the adult phase is marked by long-distance and abrupt movements, the nymph phase is characterized by short steps and gradual movements [21].The phases of GOA's intensification and diversification are represented by nymph and adult movements. According to the following mathematical model [21], grasshopper swarming behavior is as follows:

$$P_x = I_x + gf_x + W_x$$

WhereP_x represents the position of the x-th grasshopper, I_x represents grasshopper social behaviour, I_x represents the effect of gravity on the x-th grasshopper, and W_x represents wind advection. Following equation can be simplified to produce the random behavior of grasshoppers as follows:

$$P_x = a_1 I_x + a_2 g f_x + a_3 w_x$$

Where [0, 1] is the range for the random values a_1,a_2 and a_3.The following is a definition of the social interaction I_x:

$$I_x = \sum_{\substack{y=1 \\ y \neq x}} I\left(ed_{xy}\right) \widehat{ed}_{xy}$$

Where,$ed_{xy} = \left|P_y - P_x\right|$ for the Euclidean distance between the x-th and y-th grasshoppers, $\widehat{ed}_{xy} = \frac{P_y - P_x}{ed_{xy}}$ for the unit vector from the x-th to the y-th grasshopper, and I for the social pressures formed by the equation:

$$I(a) = f\, e^{\frac{-a}{l}} - e^{-a}$$

Where, f and l stand for attraction length and intensity. Attraction and repulsion are two ways that grasshoppers interact socially. The following equation provides the gravitational forcegf_x:

$$gf_x = -c\hat{e}_c$$

Where$\hat{e}$ is a unit vector pointing towards the centre of the earth and c is the gravitational constant.The following equation yields the wind advectionw_x:

$$w_x = dc\hat{e}_w$$

Where$\hat{e}_w$ is a unit vector pointing in the direction of the wind and u stands for the drift constant.A grasshopper's position is updated based on its present location, its global best location, and the locations of other grasshoppers in the swarm. This aids GOA in avoiding becoming sucked into local optima.

3.4 Deep Belief Network Grasshopper optimization Algorithm (DBNGOA)

The following are the GOA's optimization steps for DBN parameters.
Initialized the population and set all the GOA parameters.
Consider the DBN training RMSE value as the fitness function, assess each individual's fitness value fit (i) based on the learning rate and number of batch learning, and then indicate the ideal individual.
Make a determination as to whether the current iteration times have reached the termination condition; if so, end the iteration and print the result; otherwise, move on to the next step.
Update each person's position and re-initialize everyone who is outside the top and lower constraints.
Update the ideal person and begin a new iteration: $x = x + 1$

4. Experiment Results and Discussion

Tensorflow, one of the newest and most comprehensive deep learning frameworks is employed, in research study. The experiment is run on a ThinkPad E450 personal notebook with an Intel Core i5-5200U CPU run at 2.20 GHz, 8 GB of memory, and no GPU acceleration.The performance of the DBNGOA-IDS model has been examined in two tests for binary classification (Normal, anomaly) and five-category classification, including Normal, DoS, R2L, U2R, and Probe. Contrast experiments are developed concurrently in order to compare with various machine learning approaches. As described in [23], research have compared the performance ofj48, NB, RF, MLP, SVM and RNN, DNN, DBN, LSTM, CNN, BLSTM, BAT and BAT-MC with proposed DBNGOA as shown in figure 2-4.

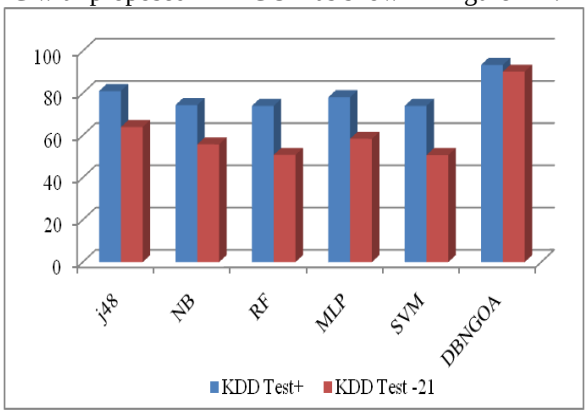

Figure 2.Performance of DBNGOA with other ML approaches

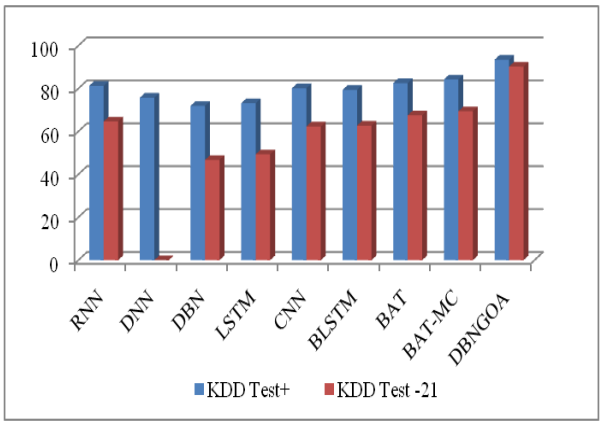

Figure 3.Performance of DBNGOA with other DL approaches

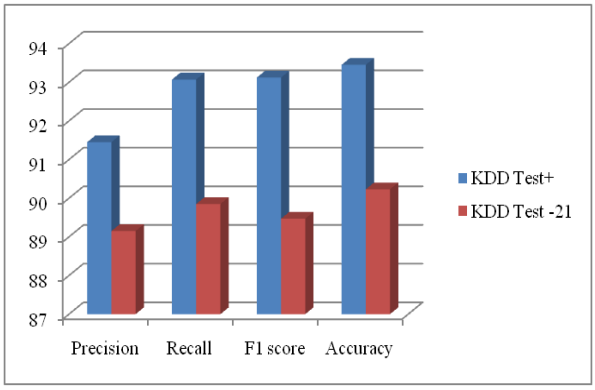

Figure 4.Performance of DBNGOA Model

Compared to traditional machine learning and deep learning approaches the proposed DBNGOA model achieved higher accuracy. The model is evaluated on both KDD Test+ and KDD Test -21 and their result is shown in figure 4. The performance metrics like precision, recall, F1 score and accuracy are calculated. The proposed model has stronger modeling ability and higher detection rate.

The experimental results demonstrate that the DBNGOA-IDS intrusion detection model, trained through the training set, has higher accuracy than the other machine learning methods and maintains a high accuracy rate. The results are based on the same benchmark, using KDD Train+ as the training set and KDD Test+ and KDDTest21 as the testing set.

5. Conclusion

The pervasive use of interconnection and interoperability in computing systems has evolved into a crucial requirement to improve daily operations. At the same time, it creates a road to vulnerabilities that can be used for malicious purposes much beyond the capacity of human control. To assume communication exchange, the weaknesses make cyber-security procedures necessary. In order to protect against threats, secure communication needs to be protected, and security measures also need to be improved in order to deal with changing security risks. In this article deep learning based adaptive and resilient network intrusion detection system (IDS) is developed to detect and classify network attacks. The DBNGOA-IDS model provides excellent modeling capabilities for intrusion detection in addition to having good accuracy.On the benchmark data set, the performance of the current study is contrasted with that of other machine learning methods. The results of the experiments show that DBNGOA-IDS outperforms conventional machine learning classification techniques in both binary and multiclass classification, and that it is especially well suited for modeling a classification model with high accuracy. The DBNGOA-IDS model offers a novel approach to intrusion detection and improves intrusion detection accuracy.

References

1. M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, ‘‘Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 3, pp. 621–636, Mar. 2018.
2. C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, ‘‘Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st Quart., 2016.
3. Yin, C., Zhu, Y., Fei, J. and He, X., 2017. A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access*, *5*, pp.21954-21961.
4. Durairaj, D., Venkatasamy, T.K., Mehbodniya, A., Umar, S. and Alam, T., 2022. Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network. *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, pp.1-23.
5. Mukherji, A., Mondal, A., Banerjee, R. and Mallik, S., 2022, December. Recent Landscape of Deep Learning Intervention and Consecutive Clustering on Biomedical Diagnosis. In *Artificial Intelligence and Applications*.
6. Verma, G.K., 2023. Multimodal Affective Computing: Affective Information Representation, Modelling, and Analysis.
7. Serey, J., Alfaro, M., Fuertes, G., Vargas, M., Durán, C., Ternero, R., Rivera, R. and Sabattin, J., 2023. Pattern Recognition and Deep Learning Technologies, Enablers of Industry 4.0, and Their Role in Engineering Research. *Symmetry*, *15*(2), p.535.
8. Sen, O., Fuad, M., Islam, M.N., Rabbi, J., Masud, M., Hasan, M.K., Awal, M.A., Fime, A.A., Fuad, M.T.H., Sikder, D. and Iftee, M.A.R., 2022. Bangla Natural Language Processing: A Comprehensive Analysis of Classical, Machine Learning, and Deep Learning Based Methods. *IEEE Access*.
9. C. Zhang, Y. He, L. Yuan and S. Xiang, "Analog Circuit Incipient Fault Diagnosis Method Using DBN Based Features Extraction," in *IEEE Access*, vol. 6, pp. 23053-23064, 2018,
10. Y. Zhang, P. Li and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," in *IEEE Access*, vol. 7, pp. 31711-31722, 2019.

11. P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li and D. Liu, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," in IEEE Access, vol. 7, pp. 87593-87605, 2019
12. Belarbi, O., Khan, A., Carnelli, P., Spyridopoulos, T. (2022). An Intrusion Detection System Based on Deep Belief Networks. In: Su, C., Sakurai, K., Liu, F. (eds) Science of Cyber Security. SciSec 2022.
13. Sajith, P.J., Nagarajan, G. Intrusion Detection System Using Deep Belief Network & Particle Swarm Optimization. Wireless Pers Commun 125, 1385–1403 (2022).
14. Balakrishnan, Nagaraj, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things." Internet of things 14 (2021): 100112.
15. Tabash, M., Abd Allah, M. and Tawfik, B., 2020. Intrusion detection model using naive bayes and deep learning technique. Int. Arab J. Inf. Technol., 17(2), pp.215-224.
16. Kalpana, R. "Recurrent nonsymmetric deep auto encoder approach for network intrusion detection system." Measurement: Sensors 24 (2022): 100527.
17. Y. N. Kunang, S. Nurmaini, D. Stiawan, A. Zarkasi, Firdaus and Jasmir, "Automatic Features Extraction Using Autoencoder in Intrusion Detection System," 2018 International Conference on Electrical Engineering and Computer Science (ICECOS), Pangkal, Indonesia, 2018, pp. 219-224.
18. G.E. Hinton, S. Osindero, and Y.W. Teh, A fast learning algorithm for deep belief nets. Neural Computation, 2006, 18(7), pp. 1527– 1554.
19. G.E. Hinton, and R.R. Salakhutdinov, 2006. Reducing the dimensionality of data with neural networks. Science, 2006, 313(5786), pp. 504-507.
20. H.Z. Wang, G.B. Wang, G.Q. Li, J.C. Peng, and Y.T. Liu, Deep belief network based deterministic and probabilistic wind speed forecasting approach. Applied Energy, 2016, 182, pp. 80-93.