Asian Journal of Research in Computer Science

9(4): 50-64, 2021; Article no.AJRCOS.69657
ISSN: 2581-8260

Deep Learning Approaches for Intrusion Detection

Azar Abid Salih[1*], Siddeeq Y. Ameen[1], Subhi R. M. Zeebaree[1], Mohammed A. M.Sadeeq[1], Shakir Fattah Kak[1], Naaman Omar[1], Ibrahim Mahmood Ibrahim[1], Hajar Maseeh Yasin[1], Zryan Najat Rashid[2] and Zainab Salih Ageed[3]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.
[2]Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq.
[3]Nawroz University, Duhok, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v9i430229
Editor(s):
(1) Dr.Shivanand S.Gornale, Rani Channamma University, India.
Reviewers:
(1) Pradeep K. V., Vellore Institute of Technology, India.
(2) Sinan Sameer Mahmood Al-Dabbagh, Al-Mansour University College, Iraq.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69657

Review Article

Received 10 April 2021
Accepted 16 June 2021
Published 17 June 2021

ABSTRACT

Recently, computer networks faced a big challenge, which is that various malicious attacks are growing daily. Intrusion detection is one of the leading research problems in network and computer security. This paper investigates and presents Deep Learning (DL) techniques for improving the Intrusion Detection System (IDS). Moreover, it provides a detailed comparison with evaluating performance, deep learning algorithms for detecting attacks, feature learning, and datasets used to identify the advantages of employing in enhancing network intrusion detection.

Keywords: Deep learning; intrusion detection; network attacks; intrusion datasets; security service.

1. INTRODUCTION

With the increasing occurrence of malicious attacks, the network's security has been essential for keeping user information safe. Many prevention and detection techniques are used to secure and network service [1,2].

However, network security management and control are challenging to protect the systems,

**Corresponding author: E-mail: azar.abid@dpu.edu.krd;*

software, devices, unauthorized data access, malware attacks, network attacks, and so on [3,4]. One of the strategies for protecting computers is building a security system to discover various types of attacks. An intrusion detection system (IDS) is an available mechanism to detect and prevent various attacks [5,6]. The concept of IDS to perform monitoring and identifying attack behavior on network traffic action [7].

A more significant gap faced by intrusion detection systems is a possibility that could be known and detect any new type of attacks. Moreover, the rapid development of information and communications technology application has created a new challenge [8,9]. With the advent of the new technology era, passing the massive amount of data from different sources on the network generated in a short time is another problem because it is not easy to detect intrusive behaviors in these large quantities of data and fast network speed [10,11].

Various methods are used to detect a suspicious attack, such as artificial intelligence and machine learning. Researchers forward to employ and investigate the deep learning method with technology development rather than traditional machine learning techniques [12-14]. Deep Learning is a modern technique for dealing with massive amounts of data that can extract useful features from big data and build models for inference, decision making, and prediction [15,16]. Deep learning approaches are applied in network intrusion detection that can uncover secret patterns and identify attacks. Furthermore, the significant point in deep learning is that it can perform feature extraction and classification tasks together [17-19]. The intrusion has different features and behaviors. One of the benefits of deep learning can automatically reduce traffic action complexity and find only relevant features among the data using feature selection and extraction [20-22]. Deep Learning has shown success in different applications. It makes daily life more efficient and intelligent, such as image processing, audio processing, video recognition, mobile devices, automation systems, robotics, etc. [23-25].

This paper discusses intrusion detection in different applications and describes the attack's type. They are also adopted in building a system for detecting malicious attacks by employing deep learning approaches. The rest of the paper is organized as follows, Section 2 Deep Learning and IDS, Section 3 Deep learning Algorithms in IDS, section 4 Discussion; finally, conclusion is presented.

2. DEEP LEARNING AND IDS

This section is broken down into four sections. The first section background for deep learning. The deep learning techniques and architecture are described in the second section. The third section discusses intrusion detection applications. The fourth section explains the network attacks, and the last section is about security datasets for computer networks.

2.1 Deep Learning

Deep Learning is advanced machine learning. It consists of multilayers and more deep layers for a Deep Neural Network (DNN) [26,27]. Deep learning is a neural network with more numbers of inputs and more complex neural layers. Machine learning is a branch of Artificial intelligence, and deep learning is a subclass of machine learning [28]. Deep learning is divided into three types of learning. The first type is supervised feature learning used for the extraction of features. These features will be supplied to straightforward machine learning methods for performing tasks such as classification and detection. The second form of unsupervised feature learning relies only on optimum feature extraction of the entire model. [29,30]. The third one is a hybrid deep using generative feature learning models to enhance the training of deep neural networks [31,32].

The advantages of deep learning include the ability to solve complicated issues, which is employed in most intelligent applications, producing the best outcomes, lowering costs, eliminating the requirement for data labeling, and training a large number of parameters [33]. Nevertheless, it also has limitations of understanding well, need for clear and big data, computationally intensive, and more complex algorithms [34,35]. The primary function of deep learning in application makes decisions, predictions, and classification. The significant point in deep learning is learning features and automatic extracting features [36].

Nowadays, depending on machine learning techniques with growing internet space and different attack features occurred unsatisfactory results. Deep learning techniques have shown their efficiency for selecting features automatically, dimensionality reduction, and classification tasks [37-39]. Deep Learning has a prominent role in application speech recognition, natural language processing, computer vision, image processing, intrusion detection, and so on [40].

2.2 Deep Learning Methods

Deep Learning is developing artificial neural networks (ANN) algorithms with many layers of neural networks [41]. The main objective of deep learning algorithms is feature learning and classification tasks [42]. Furthermore, finding correlations between features among a large amount of data. Deep learning is classified into three classes depending on architecture and techniques: discriminative is supervised, generative is unsupervised, and hybrid combining two methods, as illustrated in figure (1) [43]. In discriminative or supervised learning architectures for prediction tasks, the data are named to differentiate patterns [44]. The most popular discriminative deep learning techniques, such as a Convolutional Neural Network (CNN) this algorithm has a remarkable architecture suitable for image recognition and feature selection [43].

Unsupervised learning, also known as generative learning, employs unlabeled information; it has little training data and learns each lower layer in a layer-by-layer process [45,46]. There are several methods classified as unsupervised such as Autoencoder (AE), Boltzmann machine (BM), Recurrent neural network (RNN). The deep hybrid method is the combination of generative and discriminative methods, and it takes both advantages, such as is Deep Neural Network (DNN) and Generative Adversarial Network (GAN) [47-49].

2.3 Intrusion Detection System for Applications

There are many applications and fields faced different types of attacks such as in communication networks, Internet, Web application, cloud computing and IOT applications.

2.3.1 IDS for IOT applications

Intrusion detection is one of the leading research problems in network and computer security [50]. It is the process of monitoring and analyzing network traffic to detect malicious attacks. The intrusion detection system has an essential role in many filed such as the Internet of Things (IoT), web, wireless, and cloud [51]. IoT devices need a strong IDS to deal with the different types of threats coming from different networks. IoT as the communicating devices could reach thousands of nodes

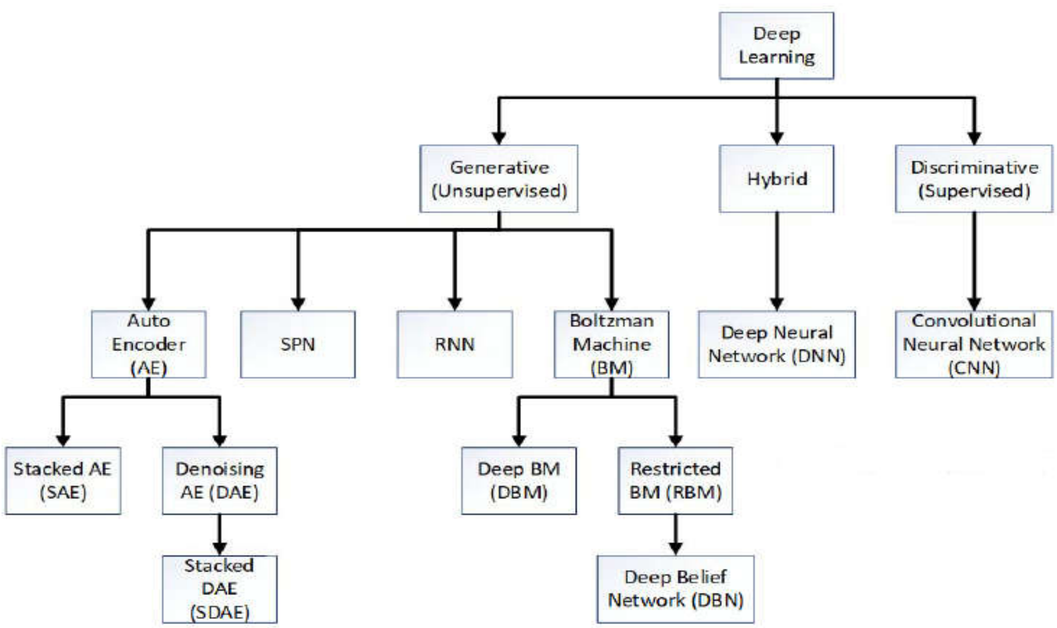

Fig. (1). Deep Learning Architecture [43]

via the internet [52,53]. There are many algorithms helps to discover different types of threats which are machine and deep learning technique to protect IoT applications. The security of devices used in many IoT applications in recent years includes smart homes, smart cities, industrial, building, retailing, and traffic [54,55]. Protecting IoT in intelligent devices needs software to capture unknown and unknown malicious attacks using different intelligent techniques [56].

2.3.2 IDS for web applications

Recently, web applications spread worldwide in different services such as shopping, bank service, and social communication [57,58]. The security of the web from various types of malicious it is needful by using anomaly detection systems. Many systems build it to secure the web, such as anomaly detection in the HTTP request parameters [59]. Simultaneously by growing internet services, the number of threats increased [60]. Although using various data sets on the attack threats that may target the web applications implemented in different intelligent techniques machine learning and deep learning, they have reported on the performance, quality, results, and protection of such attacks on their website [61,62].

2.4 Network Attacks

With expansion the communication network the world of technology need more mechanism to save systems and applications from malicious attacks. There are different ways to protect digital data from intrusion. Firstly, know information about security attack types. Secondly, security mechanism and thirdly, security services.

2.4.1 Security attacks

The detection of malicious attacks is always the primary step towards secure communication between nodes [63,64]. In everyday types of malicious attacks have been increased. There are many types of attacks classified in different cases. In general, there are two types of attacks. Firstly, an active attack tries to damage the system's resources [65,66]. This type of attack is modifying the data stream and creating false statements such as Daniel of service. Secondly, a passive attack tries to know or use the information on the system but does not damage system resources and monitoring of transmission [67-69].

2.4.2 Security Mechanism

There are various solutions available for intrusion detection and prevention in the network.

The Different security mechanisms can be used to enforce the security properties defined in a given security policy [70-72]:

Attack Prevention: The firewall prevents attacks from the outside against the machines in the inside network by denying the attempt to contact an unauthorized person [73,74]. The authentication process usually allows the user to enter the system requires a name and a password plaintext to hide its substance [75,76].

Attack Avoidance: The encryption process disguises a message depending on some transformation rules into a format that hides its substance.

Attack Detection: The most crucial technique for protecting data and systems integrity from outside intruders is intrusion detection.

2.4.3 Security Services

Intrusion detection systems (IDS) are an effective security technology that can detect and react to the attack. It performs monitoring network traffic [77,78].

An Intrusion prevention system (IPS) is a device or software that has the working as an intrusion detection system for analyzing and monitoring network traffic and malicious attack prevention and stops the possible action of attacks [79,80].

2.5 Intrusion Detection Dataset

An intrusion detection dataset can be established by collecting network traffic features from different sources, such as network traffic flows containing information about the host, user behavior, and system configurations [81-83]. This information is required to study the attack patterns and abnormal activity of various network attacks. A massive amount of data gets produced every day, and it is essential to transmit private data securely [84-86]. It is a significant data era. The administrative organization of computer security collected various features in an extensive data set. This dataset contains a considerable number of features of different types of attacks. Deep Learning is a key for extracting and reducing irrelevant features and decreasing data space [87-90].

The researcher has been conducting using different data sets the intelligent techniques to play an important role in developing computer security. Many security datasets used for intrusion detection classification as a normal and malicious attack depended on attack features such as KDD CUP99, NSL-KDD. CIDS 2017, Kyoto 2006+, CICIDS 2017, ECML-PKDD 2007, ECML-PKDD 2007, HTTP CSIC 2010, CTU-13, ADFA, UNSW-NB15. However, the most popular datasets in the research community use KDD99 and NSL-KDD because they contain the most important features to detect attacks. Moreover, researchers' most serious difficulties obtaining real-time system traffic action [91-94].

3. DEEP LEARNING ALGORITHMS IN IDS

Deep learning algorithms by many researchers focused on IDS problems because of their ability to analyze and discover useful information from large volumes of data. Therefore, different deep learning techniques have been used for intrusion detection systems. The main objective of deep learning in building intrusion systems is extraction features and classification tasks. The most popular deep learning techniques used for intrusion detection are Auto- Encoder (AE), Recurrent Neural Networks (RNN), Deep Belief Networks (DBN), Convolutional Neural Network (CNN), and Hybrid Deep Learning [95].

Every day the deep learning in progressive and new technique method occurs. As shown in Table 1, feature learning, classification intrusions detailed descriptive and comparative analysis of the published deep learning-based intrusion detection researches. The classification technique depended on the dataset used for training and testing the model, applied deep learning architecture.

3.1 Generative Architectures

Deep learning approaches can be applied to unsupervised learning. This is an important benefit because unlabeled data are more numerous than the labeled data.

3.1.1 Auto-Encoder (AE)

Auto-Encoder (AE) is the most method described in the literature, this type of method is used for dimensionality reduction and classification tasks. The function of this method the input encodes copy to output decoder. It is used in many applications feature compression and classification features. Several AE extensions include stacked AE (SAE), sparse AE, and de-noising AE [96].

In 2020 Schwartz F. et al. [97] focused on dimension reduction to reduce complicated and reducing time for building model. An autoencoder (AE) is a deep neural network used to reduce the big data with, Autoencoder (SAE) for feature extraction to reduce the feature space. The data preprocessing stage and data normalization applied to the KDD99 data set. Furthermore, three classification algorithms are Decision Trees, Naive Bayes, and Decision Table to classify data streams. They first tested the model with all 41 features without using (AE) deep learning and second-time use feature reduction methods with five and thirteen features. The experiments showed that get the best result when used decision tree classifier with 13 features. A system evaluated depended on three criteria: the accuracy of 98.2162%, the false positives 0.0066%, and the false negatives 0.0180%.

In 2019 B. Alsughayyir et al. [98] presented AE for classification tasks. In the data preprocessing stage, the Min-Max normalization is used. This model has been applied to NSL KDD dataset for the training model. The proposed model's performance gets the best results compared to traditional machine learning techniques with an accuracy of 91.28%.

In 2018 Farahnakian and Heikkonen [99] proposed Deep Auto-Encoder (DAE) for feature learning and the softmax classifier in the last hidden layer used. The model was trained on 10% of the KDD99 dataset with all the features. The proposed model gets an accuracy of 94.71% to overcome the problem of overfitting.

In 2020 Yeom et al. [100] presented AutoEncoder deep learning technique for feature extraction and classification used a random forest algorithm. This technique, by extracting some features, reduces the time and complexity. The proposed model is trained on CICIDS 2017 data set. The evaluation performance showed that the proposed AE-RF achieves an accuracy of 98%.

3.1.2 Recurrent Neural Networks (RNN)

A recurrent network is a type of ANN used for classification and regression. There are two popular types used for RNN: Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU). This type of deep learning implementing time-series data prediction. In RNN, have the edges fed into the next time step to predict. It needs to access previous information in current iterations. He was, moreover, used in many applications such as robot control, speech recognition, intrusion detection. The number of studies explored that the employed of RNN in intrusion detection gets satisfactory results [101].

In 2018, Sara et al. [102], Presented Long-Short-Term Memory LSTM using four neural networks. In this study, memory manipulations in the cells are done by gates. LSTM uses three gates: output gate, input gate, forget gate. The proposed model is applied to the CIDDS dataset. This research achieves a sufficient accuracy of 0.85.

In 2020 Al-Emadi Al. et al. [103] designed an intelligent system for cyber-attack detection using deep learning Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN). This work methodology in sequences starting from data preprocessing, feature selection, and the last step is classification attacks by deep learning. The deep learning RNNs algorithm, the Long Short-Term Memory (LSTM), and the Gated Recurrent Units (GRU) create a robust intrusion detection system. The results found that CNN has to outperform compared with RNN and other techniques with metric measurements accuracy, F1 score, recall, and precision above 97% obtained.

In 2018 Kasongo and Yanxia Sun [104] proposed a Deep Long Short-Term Memory (DLSTM) based classifier for wireless intrusion detection system (IDS). The Information Gain (IF) used as a filter select more informative features. The model is trained on NSL-KDD Dataset. The proposed model is compared with different machine learning techniques. The illustrated result showed that accuracy on validation data was 99.51%.

3.1.3 Deep Belief Networks (DBN)

Deep Belief Network (DBN) contains stacked f multiple Restricted Boltzmann Machine (RBM) methods. DBN Includes learning a probability distribution from an original dataset and making inferences about unseen data. Moreover, DBN is used for dimensionality reduction, classification, and regression tasks. The aim of DBN represents to achieve better feature learning. Each hidden layer is individually trained to rebuild the inputs by adjusting weights and fast algorithms in the training phase [105].

In 2019, Peng. X. et al. [106] presented a network intrusion detection system based on a deep learning algorithm. This system is used for feature extraction deep confidence neural network (DBN) and Back Propagation (BP) neural network classifier. The performance of the intrusion detection system evaluated using the KDD CUP'99 dataset. Data transformation needs for character type features must be numerical Features. Data normalized because the dataset contains extensive data. The analysis of feature learning methods DBN result compared with PCA and gain ratio. The result concludes that the DBN-based feature learning algorithm is more convenient for feature learning tasks in high-dimensional with s4 get high accuracy of 95.45%.

In 2019 Wei et al. [107] presented an optimization algorithm based on a deep belief network. This study used particle swarm optimization (PSO), genetic algorithm optimization back propagation (BP) PSO (GA-PSO) algorithm, and an artificial fish swarm algorithm. The proposed model was implemented on the NSLKDD dataset for the training and testing model. The results of the proposed model illustrated an accuracy of 83.86%.

In 2019 Dai and Pan [108] proposed an intrusion detection system based on improving Deep Belief Network (DBN) and Extreme Learning Machine (ELM) for classification. DBN-ELM method that used DBN to train features on NSL-KDD data set. The excremental result showed that the proposed model gets an accuracy of 97.82%.

3.2 Discriminative Architectures

Discriminative method denotes to a class of models used supervised learning data labeled especially in classification task.

3.2.1 Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) is a discriminative (supervised) learning data labeled to classify different patterns. CNN improves the connections between DNN layers. CNNs train multiple layers with nonlinear, fully connected networks. The hidden layers of a CNN consist of complex layers that convolve with multiplication or other product. The input CNN requires numeric [109]. Furthermore, CNN is used to extract dealing with more complex features to perform the task with better accuracy [110]. Many applications implementing by CNN, such as intrusion detection, identify the face, image feature extraction, and video analysis.

In 2019, Xiao X. and et al.[111], presented Convolutional Neural Network (CNN–IDS), one of the deep learning classification algorithms. They focused on the effects of dimension reduction for enhancing classification algorithms and reduce the model time training. The most important phase to build the model is data preprocessing in the data set. It starts by removing redundant and irrelevant features in the network traffic data. They used two-dimensionality reduction methods: principal component analysis (PCA) and auto-encoder (AE) on the KDD-CUP99 dataset. The feature with the analogy, the 41-feature dataset becomes 121 features and features assigned the values of 64, 81, 100, and 121 it needs to reduce the complexity and time model training. The experimental to evaluate the performance of the proposed shows the efficiently detects network intrusion by dimensionality reduction. AC, DR, and FAR can access 94.0%, 93.0%, and 0.5%. The second part of the study compares with traditional machine learning techniques such as SVM, Logistic Regression, Decision Tree, Naive Bayes Random Forest, and Adaboost.

In 2019 Lin and et al. [112] proposed convolutional neural networks (CNNs) with five layers network for extract features. The softmax used for the classification of different types of attacks. The results illustrated model get high accuracy 97.53% applied on KDD99 dataset.

In 2019 Yong and Bo [113] presented a convolutional neural network. CNN improved by Batch normalization algorithm to reduce the complexity of data and increase the model's speed in the training phase. The proposed method was applied to KDD-Cup 99 data. The results showed that the model gets high accuracy of 94.11%.

In 2019 Zeng et al. [114] proposed a system to classify and identify using several deep learning models. They adopted three deep learning models CNN, LSTM, and tacked autoencoder, to derive features from various points of view. In this app, the CNN extracted features from local features, the RNN extracted time series features, and the stacked autoencoder extracted features of the sentence. The automatic solution is working well! It currently has a perfect score on the ISCX 2012 test set. Extracting and extracting the noisiest features of an imaging feature is also a successful algorithm detection tool.

3.3 Hybrid Deep Learning

Hybrid architectures incorporate both generative and discriminative models. A hybrid deep learning model that usefully combines different deep learning methods (LSTM with GRU, BiLSTM, and CNN with other techniques). This learning under progressive and obtained the highest result various techniques use extracts features of different deep learning methods combines these features and classifies [115].

In 2018 Ludwig [116] proposed an ensemble method consists of an autoencoder, a deep belief neural network, a deep neural network, and an extreme learning machine for the classification task. The NSL-KDD dataset applied to the training model the proposed model illustrated accuracy 93%.

In 2020 Malik et al. [117] proposed Cuda-enabled is hybrid deep learning used Long short-term memory (LSTM) and Convolutional Neural Network (CNN) for efficient and timely detection of multi-vector threats and attacks. The CICIDS2017 data set used and obtained performance is 98.6% detection accuracy.

In 2020, Zhang et al. [118], Proposed an ensemble Bayesian Convolutional Neural Network to build an intrusion detection system. Both data sets, NSL-KDD and UNSW-NB15, are used to evaluate the proposed schemes. Ensemble-based detection model gets high accuracy with data set NSL-KDD in term accuracy 99.3271%.

In 2020 Atefi and H. et al. [119] proposed a hybrid classification method Deep Learning (DL) and Binary Algorithms (BA), combined for IDS. In another hand of this work introduced Deep Neural Network (DNN) and Binary Genetic Algorithm (BGA), Binary Bat Algorithm (BBA), Binary Gravitational Search Algorithm (BGSA) as best fit model to increase the rates of detection. The genetic algorithms select more than eighty features from network flow. The result displayed

Table 1. Performance of deep learning approaches for intrusion detection system

Ref	Data set	Feature learning and selection	Algorithms detect attacks	Accuracy description
[64] 2020	KDD'99	feature reduction AE FE and SAE	decision trees, Naive Bayes , decision tables	Best result 13 features, accuracy 98.2162. FP 0.0066% , FN 0.0180%
[65] 2018	NSL-KDD		AE	Multi-class accuracy-99%.
[66] 2019	KDD99	SAE	Softmax	Multi-classification Accuracy 94.71%
[67] 2019	CICIDS 2017	AE	Random forest	accuracy of 98%.
[69] 2018	CIDDS		LSTM	accuracy 85%
[70] 2020	NSL-KDD	LSTM GURU	CNN RNNs	CNN rate for recall, F1 score, and precision of above 97%
[71] 2020	KDD	Information Gain	DLSTM	accuracy 99.51%,
[73] 2019	KDD CUP'99	DBN	BP neural network	DBN with S4 get high accuracy 95.45%
[74] 2019	NSL-KDD	DBN	PSO -AFS-GA - BP	accuracy 82.36%
[75] 2019	NSL-KDD	DBN	DBN-ELM	accuracy 97.82%
[78] 2019	KDD-CUP99	CNN dimension reduction with PCA, AE	Softmax classifier	accuracy 94.0%
[79] 2019	KDD99	CNN	Softmax	accuracy 97.53%
[80] 2019	KDD CUP 99	CNN With Batch normalization	-	accuracy 94.1
[81] 2019	ISCX 2012	CNN, an LSTM, and SAE	DFR	accuracy 99.22%
[83] 2018	NSL-KDD	ensemble method - AE, DBF, deep NN, and ELM		precision 92%
[84] 2020	CICIDS2017	LSTM CNN		accuracy 98.6%
[85] 2020	NSL -KDD UNSW-NB15	Bayesian CNN		Accuracy 99.3271 NSL -KDD UNSW-NB15 98.6833
[86] 2020	CICIDS2017	GA selection	DNN with BBA, DNN with BGA, DNN with BGSA	Higher score DNN with BGSA accuracy 99.002
[87] 2018	NSL-KDD		DL built using H2O, Naive Bayes, SVM, Random Forest, and Logistic Regression	DL get a high accuracy rate Binary Classification accuracy 83,87%,Multiple Classification accuracy 84,13%

that the BGSA gets the best performance of the hybrid method inaccuracy 99.002, recall 99.02, precision 98.98, sensitivity 99.022%, specificity 98.984, and cost error 0.997%. The proposed model was applied to a new dataset named CICIDS2017.

In 2018, Santhosh and A. M [120] proposed the real-time IDS based on the cloud using deep learning and machine learning algorithms. In deep learning, building models using H2O and deep learning 4J libraries to classify data as binary and multinomial classes. Also, in machine learning for classification using Support Vector Machine, Random Forest, Logistic Regression, and Naive Bayes algorithms. The IDS detection 99.5% accuracy for the training phase and 83% accuracy on the test phase applied to the NSL-KDD dataset. They compared results between machine learning algorithms and deep learning, showing that the choice of deep learning for binomial and multinomial classification gets the best accurate detection and fast training model for IDS. However, use multiclass Prob, Dos, R2L, and U2R for classifying intrusion detection. The accuracy of binary classification 83,87%, and Multi classification accuracy 84,13%.

4. COMPARISON AND DISCUSSION

This paper considers implementing deep learning techniques between 2018 and 2020, as shown in Table (1), to evaluate the performance of different approaches to enhancing intrusion detection systems. Previous sections reviewed some research about deep learning methods applied to build IDS. Deep Learning is employed to improve network intrusion detection systems (NIDS) in identifying different malicious attacks.

Intrusion detection system dealing with a massive amount of features. The primary role of the deep learning method is feature learning by reducing the complexity of big data sets. Furthermore, data preprocessing feature extraction is not used in deep learning. The AE generative model has been primarily used for feature learning with high accuracy. The performance of the classification task using deep learning techniques achieved high detection accuracy. The RNN is mainly used as a classification for different types of attacks that obtained high results.

The hybrid deep learning and called ensemble learning approaches are a progressive method, and it takes excellent properties of each group of the algorithm because intrusion detection faced many cases problem with dealing different big data, so by combining different algorithms could ability fill the gaps of model and get the best results. The comparison among different deep learning techniques is conducted to show the efficiency of deep learning in intrusion detection. On the other hand, deep learning takes a long time in the building model's training phase and needs high machine storage. Deep learning displays substantial advantages in feature extraction. It has been widely used in the field of feature selection and gradually replaced traditional machine learning algorithms. The enhancement of the intrusion detection system depended on detection and classification accuracy. In evaluating the performance of deep learning algorithms based on different metrics, most of the researchers focused on accuracy as the primary metric.

In this paper, the comparison is performed in the data set, feature learning techniques, deep learning algorithm. This study aims to show the performance of different profound learning algorithms results is given in Table 1.

5. CONCLUSION

Deep learning algorithms are highly effective in developing an intrusion detection system (IDS) for detecting different types of attacks. The main objective of using deep learning methods can be used in anomaly detection for both processes dimensionality reduction and classification tasks. Furthermore, it performs better and deals with complex big data sets than traditional machine learning algorithms. This paper reviewed many works and concluded that the hybrid deep learning method is increasingly employed to detect threats with high accuracy.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Shrestha A, Mahmood A. "Review of deep learning algorithms and architectures," IEEE Access. 2019;7:53040-53065.
2. Hassan RJ, Zeebaree SR, Ameen SY, Kak SF, Sadeeq MA, Ageed ZS, et al., "State of art survey for iot effects on smart city technology: Challenges, opportunities, and

solutions," Asian Journal of Research in Computer Science. 2021;32-48.
3. TabassumA, Erbad A, Guizani M. "A survey on recent approaches in intrusion detection system in iots," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). 2019;1190-1197.
4. Yasin HM, Zeebaree SR, Sadeeq MA, Ameen SY, Ibrahim IM, Zebari RR, et al. "IoT and ICT based Smart Water Management, Monitoring and Controlling System: A Review," Asian Journal of Research in Computer Science. 2021;42-56.
5. Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaee M, Karimipour H. "Cyber intrusion detection by combined feature selection algorithm," Journal of Information Security and Applications. 2019;44:80-88,
6. Abdullah SMSA, Ameen SYA, Sadeeq MA, Zeebaree S. "Multimodal emotion recognition using deep learning," Journal of Applied Science and Technology Trends. 2021;2:52-58.
7. Kaja N, Shaout A, Ma D, "An intelligent intrusion detection system," Applied Intelligence. 2019;49:3235-3247.
8. Duić I, Cvrtila V, Ivanjko T. "International cyber security challenges," in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2017;1309-1313.
9. Sallow A, Zeebaree S, Zebari R, Mahmood M, Abdulrazzaq M, Sadeeq M. "Vaccine tracker," SMS reminder system: Design and implementation; 2020.
10. Dong Y, Wang R, He J. "Real-time network intrusion detection system based on deep learning," in 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS). 2019;1-4.
11. Janaby AOAL, Al-Omary A, Ameen SY, Al-Rizzo HM. "Tracking high-speed users using SNR-CQI Mapping in LTE-A Networks," in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). 2018;1-7.
12. Fernández GC, Xu S. "A case study on using deep learning for network intrusion detection," in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). 2019;1-6.
13. Othman A, Ameen SY, Al-Rizzo H. "Dynamic Switching of Scheduling Algorithm for," International Journal of Computing and Network Technology. 2018;6.
14. Jijo BT, Zeebaree SR, Zebari RR, Sadeeq MA, Sallow AB, Mohsin S, et al. "A comprehensive survey of 5G mm-wave technology design challenges," Asian Journal of Research in Computer Science. 2021;1-20.
15. Shashank K, Balachandra M. "Review on network intrusion detection techniques using machine learning," in 2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER). 2018;104-109.
16. Kareem FQ, Zeebaree SR, Dino HI, Sadeeq MA, Rashid ZN, Hasan DA, et al. "A survey of optical fiber communications: challenges and processing time influences," Asian Journal of Research in Computer Science. 2021;48-58.
17. Mighan SN, Kahani M. "Deep learning based latent feature extraction for intrusion detection," in Electrical Engineering (ICEE), Iranian Conference on. 2018;1511-1516.
18. Omer MA, Zeebaree SR, Sadeeq MA, Salim BW, Mohsin SX, Rashid ZN, et al. "Efficiency of malware detection in android system: A survey," Asian Journal of Research in Computer Science. 2021;59-69.
19. Ameen SY, Nourildean SW. "Coordinator and router investigation in IEEE802. 15.14 ZigBee wireless sensor network," in 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE). 2013;130-134.
20. He Z, Peng Y, Zhao Y, Yang J, Wang L, Zheng B, et al. "Deep learning-based automatic modulation recognition algorithm in non-cooperative communication systems," in 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP). 2019;1-6.
21. Ameen SY, Ali ALSH. "A Comparative Study for New Aspects to Quantum Key Distribution," Journal of Engineering and Sustainable Development. 2018;11:45-57.
22. Jacksi K, Ibrahim RK, Zeebaree SR, Zebari RR, Sadeeq MA. "Clustering Documents based on Semantic Similarity using HAC and K-Mean Algorithms," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;205-210.

23. Wang J, Cao B, Yu P, Sun L, Bao W, Zhu X. "Deep learning towards mobile applications," in 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). 2018;1385-1393.
24. Fawzi LM, Ameen SY, Alqaraawi SM, Dawwd SA. "Embedded real-time video surveillance system based on multi-sensor and visual tracking," Appl. Math. Infor. Sci. 2018;12:345-359.
25. Elzanati WM, Ameen SY. "Cost effective air-conditioning for bahrain domestic applications," in 2013 7th IEEE GCC Conference and Exhibition (GCC). 2013;535-540.
26. Modi AS. "Review article on deep learning approaches," in 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). 2018;1635-1639.
27. Sadeeq MA, Abdulazeez AM. "Neural Networks Architectures Design, and Applications: A Review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;199-204.
28. Shinde PP, Shah S. "A review of machine learning and deep learning applications," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). 2018;1-6.
29. Hallett N, Yi K, Dick J, Hodge C, Sutton G, Wang YG, et al. "Deep learning based unsupervised and semi-supervised classification for keratoconus," in 2020 International Joint Conference on Neural Networks (IJCNN). 2020;1-7.
30. Ameen SY, Al-Badrany MR. "Optimal image steganography content destruction techniques," in International Conference on Systems, Control, Signal Processing and Informatics. 2013;453-457.
31. Masita KL, Hasan AN, Shongwe T. "Deep learning in object detection: A review," in 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD). 2020;1-11.
32. Ameen SY, Ahmed IM. "Design and implementation of e-laboratory for information security training," in 2013 Fourth International Conference on e-Learning" Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity". 2013:310-317.
33. Aziz ZAA, Ameen SYA. "Air pollution monitoring using wireless sensor networks," Journal of Information Technology and Informatics. 2021;1:20-25.
34. Amanuel SVA, Ameen SYA. "Device-to-device communication for 5G security: A review," Journal of Information Technology and Informatics. 2021;1:26-31,
35. Ali ZA, Ameen SY. "Detection and prevention cyber-attacks for smart buildings via private cloud environment," International Journal of Computing and Network Technology. 2018;6:27-33.
36. Ünal Z. "Smart Farming Becomes Even Smarter With Deep Learning—A Bibliographical Analysis," IEEE Access. 2020;8:105587-105609.
37. Hatcher WG, Yu W. "A survey of deep learning: Platforms, applications and emerging research trends," IEEE Access. 2018;6:24411-24432.
38. Fawzi LM, Ameen SY, Dawwd SA, Alqaraawi SM. "Comparative study of ad-hoc routing protocol for oil and gas pipelines surveillance systems," International Journal of Computing and Network Technology. 2016;4.
39. Ghonaimy MA, El-Hadidi MT, Aslan HK. Security in the information society: Visions and perspectives Springer. 2012;86.
40. Fink O, Wang Q, Svensén M, Dersin P, Lee W-J, Ducoffe M. "Potential, challenges and future directions for deep learning in prognostics and health management applications," Engineering Applications of Artificial Intelligence. 2020;92:103678.
41. Abdullah DM, Ameen SY. "Enhanced mobile broadband (EMBB): A review," Journal of Information Technology and Informatics. 2021;1:13-19.
42. Chen M, Challita U, Saad W, Yin C, Debbah M. "Artificial neural networks-based machine learning for wireless networks: A tutorial," IEEE Communications Surveys & Tutorials. 2019;21:3039-3071.
43. Kim K, Aminanto ME. "Deep learning in intrusion detection perspective: Overview and further challenges," in 2017 International Workshop on Big Data and Information Security (IWBIS). 2017;5-10.
44. Khalid LF, Ameen SY. "Secure Iot Integration In daily Lives: A Review," Journal of Information Technology and Informatics. 2021;1:6-12.
45. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo H. "Tracking and controlling high-

speed vehicles via CQI in LTE-A systems," International Journal of Computing and Digital Systems. 2020;9:1109-1119.

46. Farhan FY, Ameen SY. "Improved hybrid variable and fixed step size least mean square adaptive filter algorithm with application to time varying system identification," in 2015 10th System of Systems Engineering Conference (SoSE). 2015;94-98.
47. Kim K, Aminanto ME, Tanuwidjaja HC. "Deep Learning-Based IDSs," Network Intrusion Detection using Deep Learning. 2018;35-45.
48. Zeebaree S, Ameen S, Sadeeq M. "Social media networks security threats, risks and recommendation: A case study in the kurdistan region," International Journal of Innovation, Creativity and Change. 2020;13:349-365.
49. Othman A, Ameen SY, Al-Rizzo H. "A new channel quality indicator mapping scheme for high mobility applications in LTE systems," Journal of Modeling and Simulation of Antennas and Propagation. 2015;1:38-43.
50. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, Adel A-Z, et al. "Comprehensive Survey for Cloud Computing Based Nature-Inspired Algorithms Optimization Scheduling," Asian Journal of Research in Computer Science. 2021;1-16.
51. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Rashid ZN, Salih AA, et al. "A survey of data mining implementation in smart city applications," Qubahan Academic Journal. 2021;1:91-99.
52. Anthi E, Williams L, Burnap P. "Pulse: An adaptive intrusion detection for the internet of things,"; 2018.
53. Ageed ZS, Zeebaree SR, Sadeeq MA, Abdulrazzaq MB, Salim BW, Salih AA, et al. "A state of art survey for intelligent energy monitoring systems," Asian Journal of Research in Computer Science. 2021;46-61.
54. Jain V, Agrawal M. "Applying genetic algorithm in intrusion detection system of iot applications," in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). 2020;284-287.
55. Abdulqadir HR, Zeebaree SR, Shukur HM, Sadeeq MM, Salim BW, Salih AA, et al. "A study of moving from cloud computing to fog computing," Qubahan Academic Journal. 2021;1:60-70.
56. Li J, Zhao Z, Li R, Zhang H. "Ai-based two-stage intrusion detection for software defined iot networks," IEEE Internet of Things Journal. 2018;6:2093-2102.
57. Salih AA, Abdulazeez AM. "Evaluation of classification algorithms for intrusion detection system: A review," Journal of Soft Computing and Data Mining. 2021;2:31-40.
58. Zebari SR, Yaseen NO. "Effects of Parallel Processing Implementation on Balanced Load-Division Depending on Distributed Memory Systems," J. Univ. Anbar Pure Sci. 2011;5:50-56.
59. Dmitry D, Elena P, Anna C, Tatiana Z, Elena P. "Approaches to anomaly detection in web application intrusion detection systems," in 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2020;532-535.
60. Shukur H, Zeebaree S, Zebari R, Zeebaree D, Ahmed O, Salih A. "Cloud computing virtualization of resources allocation for distributed systems," Journal of Applied Science and Technology Trends. 2020;1:98-105.
61. Sharma S, Zavarsky P, Butakov S. "machine learning based intrusion detection system for web-based attacks," in 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2020;227-230.
62. Abdulla AI, Abdulraheem AS, Salih AA, Sadeeq MA, Ahmed AJ, Ferzor BM, et al., "Internet of Things and Smart Home Security," Technol. Rep. Kansai Univ. 2020;62:2465-2476.
63. Abdulraheem AS, Salih AA, Abdulla AI, Sadeeq MA, Salim NO, Abdullah H, et al. "Home automation system based on IoT,"; 2020.
64. Othman A, Ameen SY, Al-Rizzo H. "An Energy-Efficient MIMO-Based 4G LTE-A Adaptive Modulation and Coding Scheme for High Mobility Scenarios," International Journal of Computing and Network Technology. 2015;3.
65. Salih AA, Zeebaree SR, Abdulraheem AS, Zebari RR, Sadeeq MA, Ahmed OM. "Evolution of Mobile Wireless Communication to 5G Revolution," Technology Reports of Kansai University. 2020;62:2139-2151.

66. Ameen SY, Nourildean SW. "Firewall and VPN investigation on cloud computing performance," International Journal of Computer Science and Engineering Survey. 2014;5:15.
67. Kandan AM, Kathrine GJ, Melvin AR. "Network Attacks and Prevention techniques-A Study," in 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). 2019;1-6.
68. Vegda H, Modi N. "Secure and efficient approach to prevent ad hoc network attacks using intrusion detection system," in 2018 Second international conference on intelligent computing and control systems (ICICCS). 2018;129-133.
69. Salih AA, Abdulrazaq MB. "Combining best features selection using three classifiers in intrusion detection system," in 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019;94-99.
70. Kruegel C, Valeur F, Vigna G. Intrusion detection and correlation: Challenges and solutions Springer Science & Business Media. 2004;14.
71. Nada JA, Al-Mosa MR. "A proposed wireless intrusion detection prevention and attack system," in 2018 International Arab Conference on Information Technology (ACIT). 2018;1-5.
72. Yazdeen AA, Zeebaree SR, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," Qubahan Academic Journal. 2021;1:8-16.
73. Abdulrazaq M, Salih A. "Combination of multi classification algorithms for intrusion detection system," Int. J. Sci. Eng. Res. 2015;6:1364-1371.
74. Hamed ZA, Ahmed IM, Ameen SY. "Protecting Windows OS Against Local Threats Without Using Antivirus," relation. 2020;29:64-70.
75. Dino HI, Zeebaree SR, Salih AA, Zebari RR, Ageed ZS, Shukur HM, et al. "Impact of Process Execution and Physical Memory-Spaces on OS Performance."; 2015.
76. Ameen SY. "Advanced Encryption Standard (AES) Enhancement Using Artificial Neural Networks," Int J of Scientific & Engineering Research. 2014;5.
77. Ahmed MRA-G, Ali FMA. "Enhancing Hybrid Intrusion Detection and Prevention System for Flooding Attacks Using Decision Tree," in 2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE). 2019;1-4.
78. Al-Khayat ON, Ameen SY, Abdallah MN. "WSNs Power Consumption Reduction using Clustering and Multiple Access Techniques," International Journal of Computer Applications. 2014;87.
79. Chandre PR, Mahalle PN, Shinde GR. "Machine learning based novel approach for intrusion detection and prevention system: A tool based verification," in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). 2018;135-140.
80. Mohammed K, Ameen S. "Performance investigation of distributed orthogonal space-time block coding based on relay selection in wireless cooperative systems."; 2019.
81. Thakkar A, Lohiya R. "A review of the advancement in intrusion detection datasets," Procedia Computer Science. 2020;167;636-645.
82. Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. "Two Levels Alert Verification Technique for Smart Oil Pipeline Surveillance System (SOPSS)," International Journal of Computing and Digital Systems. 2019;8:115-124.
83. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Yahia HS, Mahmood MR, et al., "Comprehensive survey of big data mining approaches in cloud systems," Qubahan Academic Journal. 2021;1:29-38.
84. Al-Sultan MR, Ameen SY, Abduallah WM. "Real Time Implementation of Stegofirewall System," International Journal of Computing and Digital Systems. 2019;8:498-504.
85. Abdulrahman LM, Zeebaree SR, Kak SF, Sadeeq MA, Adel A-Z, Salim BW, et al. "A state of art for smart gateways issues and modification," Asian Journal of Research in Computer Science. 2021;1-13.
86. Malallah H, Zeebaree SR, Zebari RR, Sadeeq MA, Ageed ZS, Ibrahim IM, et al. "A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems," Asian Journal of Research in Computer Science. 2021;16-31.
87. Zhong W, Yu N, Ai C. "Applying big data based deep learning system to intrusion detection," Big Data Mining and Analytics. 2020;3:181-195.

88. Haji SH, Zeebaree SR, Saeed RH, Ameen SY, Shukur HM, Omar N, et al. "Comparison of Software Defined Networking with Traditional Networking," Asian Journal of Research in Computer Science. 2021;1-18.
89. Ibrahim IM. "Task scheduling algorithms in cloud computing: A review," Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12:1041-1053.
90. Zebari IM, Zeebaree SR, Yasin HM. "Real Time Video Streaming From Multi-Source Using Client-Server for Video Distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
91. Ahmim A, Maglaras L, Ferrag MA, Derdour M, Janicke H. "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). 2019;228-233.
92. Yavanoglu O, Aydos M. "A review on cyber security datasets for machine learning algorithms," in 2017 IEEE International Conference on Big Data (Big Data). 2017;2186-2193.
93. Yasin HM, Zeebaree SR, Zebari IM. "Arduino Based Automatic Irrigation System: Monitoring and SMS Controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
94. Zeebaree S, Yasin HM. "Arduino based remote controlling for home: Power saving, security and protection," International Journal of Scientific & Engineering Research. 2014;5:266-272.
95. Wu P, Guo H. "LuNET: A deep neural network for network intrusion detection," in 2019 IEEE Symposium Series on Computational Intelligence (SSCI). 2019;617-624.
96. Wu D, Nekovee M, Wang Y. "Deep Learning-Based Autoencoder for m-User Wireless Interference Channel Physical Layer Design," IEEE Access. 2020;8:174679-174691.
97. Schuartz FC, Fonseca M, Munaretto A. "Improving threat detection in networks using deep learning," Annals of Telecommunications. 2020;1-10.
98. Alsughayyir B, Qamar AM, Khan R. "Developing a network attack detection system using deep learning," in 2019 International Conference on Computer and Information Sciences (ICCIS). 2019;1-5.
99. Farahnakian F, Heikkonen J. "A deep auto-encoder based approach for intrusion detection system," in 2018 20th International Conference on Advanced Communication Technology (ICACT). 2018;178-183.
100. Yeom S, Choi C, Kim K. "AutoEncoder Based Feature Extraction for Multi-Malicious Traffic Classification,"; 2020.
101. S. Nayyar, S. Arora, and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," in 2020 International Conference on Communication and Signal Processing (ICCSP). 2020;0136-0140.
102. Althubiti SA, Jones EM, Roy K. "Lstm for anomaly-based network intrusion detection," in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC). 2018;1-3.
103. Al-Emadi S, Al-Mohannadi A, Al-Senaid F. "Using Deep Learning Techniques for Network Intrusion Detection," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). 2020;171-176.
104. Kasongo SM, Sun Y. "A deep long short-term memory based classifier for wireless intrusion detection system," ICT Express. 2020;6:98-103,
105. Tian Q, Han D, Li K-C, Liu X, Duan LA. Castiglione, "An intrusion detection approach based on improved deep belief network," Applied Intelligence. 2020;50:3162-3178.
106. Peng W, Kong X, Peng G, Li X, Wang Z. "Network intrusion detection based on deep learning," in 2019 International Conference on Communications, Information System and Computer Engineering (CISCE). 2019;431-435.
107. Wei P, Li Y, Zhang Z, Hu T, Li Z, Liu D. "An optimization method for intrusion detection classification model based on deep belief network," IEEE Access. 2019;7:87593-87605.
108. Liang D, Pan P. "Research on intrusion detection based on improved DBN-ELM," in 2019 international conference on communications, information system and computer engineering (CISCE). 2019;495-499.
109. Zhang X, Ran J, Mi J. "An intrusion detection system based on convolutional neural network for imbalanced network traffic," in 2019 IEEE 7th International Conference on Computer Science and

Network Technology (ICCSNT). 2019;456-460.
110. Praanna K, Sruthi S, Kalyani K, Tejaswi AS. "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data."; 2016.
111. Xiao Y, Xing C, Zhang T, Zhao Z. "An intrusion detection model based on feature reduction and convolutional neural networks," IEEE Access. 2019;7:42210-42219.
112. Lin W-H, Lin H-C, Wang P, Wu B-H, Tsai J-Y. "Using convolutional neural networks to network intrusion detection for cyber threats," in 2018 IEEE International Conference on Applied System Invention (ICASI). 2018;1107-1110.
113. Yong L, Bo Z. "An intrusion detection model based on multi-scale CNN," in 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). 2019;214-218.
114. Zeng Y, Gu H, Wei W, Guo Y. "$ Deep-full-range $: A deep learning based network encrypted traffic classification and intrusion detection framework," IEEE Access. 2019;7:45182-45190.
115. Salur MU, Aydin I. "A novel hybrid deep learning model for sentiment classification," IEEE Access. 2020;8:58080-58093.
116. Ludwig SA. "Applying a neural network ensemble to intrusion detection," Journal of Artificial Intelligence and Soft Computing Research. 2019;9.
117. Malik J, Akhunzada A, Bibi I, Imran M, Musaddiq A, Kim SW. "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN," IEEE Access. 2020;8:134695-134706.
118. Zhang J, Li F, Ye F. "An Ensemble-based Network Intrusion Detection Scheme with Bayesian Deep Learning," in ICC 2020-2020 IEEE International Conference on Communications (ICC). 2020;1-6.
119. Atefi K, Hashim H, Khodadadi T. "A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)," in 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA). 2020;29-34.
120. Parampottupadam S, Moldovann A-N. "Cloud-based real-time network intrusion detection using deep learning," in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018;1-8.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/69657