Intrusion Detection System Using Deep Learning Approaches: A Survey

Kantagba Edmond, Parma Nand, and Pankaj Sharma

Abstract In recent years, there has been an urge for development in network technologies and that has contributed to an increase in cyber-attacks that are threats and challenges to the protection of network resources. In contribution to the protection of the network, artificial intelligence has been shown to be an efficient and better technique used in recent years for better detection of network attacks. In the paper, we propose an overview of deep learning techniques which are applied in intrusion detection systems. A summary of different deep learning techniques and their applications in intrusion detection systems are proposed with the various problems encountered by network security. We also give a brief summary of the benchmark datasets used in the deep learning techniques and provide a comparison of the performance of the different techniques. Finally, we propose suggestions to improve the performance of those deep learning in the attack detection.

Keywords Cyber-attacks · Artificial intelligence · Intrusion detection system · Deep learning

1 Introduction

There is a large growth in internet usage due to its numerous benefits to users and organisations in the aspect of sharing resources and other activities. This large usage of the internet has led to an increase in cyber-attack targeting those networks and personal data over the internet. Attackers are always finding a new way to overcome

K. Edmond (✉) · P. Nand · P. Sharma
Sharda University, Greater Noida, Uttar Pradesh, India
e-mail: 2020826402.edmond@pg.sharda.ac.in

P. Nand
e-mail: parma.nand@sharda.ac.in

P. Sharma
e-mail: pankaj.sharma1@sharda.ac.in

D. Gupta et al. (eds.), *International Conference on Innovative Computing and Communications*, Lecture Notes in Networks and Systems 471,
https://doi.org/10.1007/978-981-19-2535-1_64

the detection and protection systems. So, it is important that individuals and institutions such as financial, governmental and educational institutions have to always deploy new ways and techniques to protect their data and resources against intelligent attacks. Ingenious has been employed in cyber-attacks to make detection difficult with standard detection systems such as intrusion detection systems that are no more efficient and unable sometimes to detect unknown and new attacks.

The intrusion detection system has attracted various researchers to work in this field over the past years and they employed several machine learning techniques especially deep learning techniques to improve IDS performances in intrusion detection systems. The traditional intrusion detection systems had some limitations such as low performance in detecting unknown and new attacks and also the confusion in classifying normal traffic as malicious. So, the use of machine learning techniques has really helped solve some of those limitations [1]. Machine learning by its ability to simulate human brain network structure has made a great breakthrough and these approaches are classified as deep learning methods to solve complex problems efficiently.

The advantages and benefits of deep learning methods have led various authors to use these methods to propose intelligent intrusion decision systems. Therefore, several researchers have proposed models using those methods in order to increase the efficiency of IDS. In this paper, we used different papers that are used as the foundation to our paper and there is a lot of literature that helped us in this paper like [2, 3]. This paper provides an explanation and summary of the application of deep learning in attacks detections and gives a comparative statistic on the performance of each method studied in this paper.

In this paper, we provide a summary of security issues in the network and then categorise the previous methods used in solving those problems. Then, the progress of the deep learning methods in attack detection and cybersecurity, in general, are introduced and in the process of solving issues related to the traditional machine learning techniques such as false reduction rate. Furthermore, a performance comparison analysis of the different deep learning algorithms with the various benchmark dataset is proposed in this paper. Finally, we summarize the different difficulties to be solved in future work to help enhance the performance of the deep learning techniques.

Section 2 gives an overview of the concepts of attack detection and Sect. 3 provides a classification of deep learning techniques used in IDS in unsupervised and supervised methods. Section 4 focuses on the datasets used and analyses the performance comparisons of the various deep learning methods. Section 5 is the last part in which we make the discussion and summary on the basis of the current foundations.

2 Overview of Attack Detection

It is necessary to briefly discuss attack detection in general as background knowledge before getting into intrusion detection using deep learning techniques. An attack is an attempt to get unauthorised access or to bypass the security mechanism or policies of a system or group of the system forming a network. The security experts or personnel are always finding means and ways to protect and avoid their resources being compromised and one of the mechanisms usually employed is the intrusion detection system.

The intrusion detection system is the process of tracking activities including network traffic, and examining them for any signal of intrusions [4]. The dramatic advances in the era particularly in wireless verbal exchange systems are leading to an increase in threats and assaults focused on greater wi-fi communications structures because of the openness of wi-fi channels [4]. The dramatic advances in technology especially in wireless communication systems are leading to an increase in threats and attacks targeting more wireless communications systems due to the openness of wireless channels. There are three different ways in which intrusion detection systems can detect a sign of intrusion which are signature-based, anomaly-based detection and stateful protocol analysis. A signature-based detection, analyse traffic by comparing patterns or strings of the traffic with the ones already present in its database to differentiate malicious traffic and normal. So, it can define that signature-based detects already known attacks. Anomaly-based detection works in monitoring the behaviour of the network or system and if there is a deviation from known or normal behaviour such as monitoring regular activities and network connections failure or the unexpected failure of the system or overwhelming uses of network resources. In this age of machine learning, IDS are developed using machine learning algorithms, especially deep learning methods, to detect various attacks such as abnormal packet attacks, flooding, spoofing and distributed denial of service.

There has been an urgent development in machine learning this recent year, and the deep learning approach with its ability to solve complex problems has gotten more attention in the detection system. Deep learning structures simulate interconnecting neurons of human brains by using artificial neural networks, which gives them the ability to solve problems that are complex to standard algorithms [5]. Several applications of deep learning structure in intrusion detection have been proposed and shown a good achievement of this structure. Due to its great potential, deep learning is widely used in cybersecurity and specific areas of applications are phishing, malware, spam detection and analysis of traffic [6]. Shone et al. [3] came up with a network intrusion detection system which uses deep learning, helpful in network traffic analysis with an asymmetrical deep autoencoder. Vinayakumar et al. [7] used the LSTM set of rules and designed an IDS approach which allows the semantics of every name and courting at the community with an integration technique for an anomaly intrusion detection machine.

3 Attack Detection Using Deep Learning Methods

Deep learning consists of different methods, each one of which helps accomplish specific problems in their ways with varied performances. The deep learning methods can be categorised into two main types such as unsupervised learning and supervised learning. The quantity of information that is manually provided by manually labelled samples to the supervised, and the supervised methods results in high accuracy compared to the unsupervised learning methods which have less knowledge from labelled samples [8]. However, in complex attacks, manually labelling data leads to time consumption and there are situations such as the inherent complexity of real-world virtual web attacks. So, in this case, unsupervised methods take advantage of supervised methods because they can perform without prior knowledge [1].

a. Review of Unsupervised Learning in intrusion Detection

- Autoencoder Based Methods

Called an information compression set of rules, Autoencoder in his function compresses the input facts into feature area illustration and then, reconstructs the representation into the output. For the reason that autoencoder is taken into consideration to be a representing mastering algorithm. It is broadly used in dimension reduction and used to symbolize ordinary behaviour which offers the advantage of dynamically representing unknown assaults in the class with its compressed characteristic space.

Yu et al. [9] have proposed a NIDS using Stacking Dilated Convolutional Autoencoders, made of representation learning and self-taught to extract informative features from authentic traffic data. Firstly, the authentic network traffic is transformed into a numeric vector which is a training dataset through the pre-processing module. Afterwards, this model learns from unlabelled samples in the unsupervised training stage. The hierarchical structure of the feature representation and the feature description ability is improved using a backpropagation algorithm and a few labels.

Furthermore, a ‘Non-Symmetric Deep Auto-Encoder model’ has been proposed by Shone et al. [3] which was constructed using the encoder phase which is a shift from the encoder-decoder architecture. With the adequate studying shape given, the model computational time can be reduced and a decrease can be noticed in the overheads, all this with less impact on efficiency and accuracy. The evaluation of their model has been carried out using KDD Cup99 and NSL-KDD datasets which showed good results compared to others.

IEEE Staff [10] introduced an intrusion detection “Deep Auto-encoder (DAEs)” that reveals essential feature representations present inside the imbalanced training data which then provides a model for abnormal and normal behaviours detection. In order to avoid overfitting, the model was trained using unsupervised learning and at the top of the model for representing the desired outputs, they made use of SoftMax. The KDD Cup99 dataset is used to implement their model and has shown high accuracy.

Autoencoder with the structure of information compression and feature generation when used in feature extraction bring the advantages of automatic and dynamic feature construction. So, autoencoder performs well with high accuracy with predefined attacks present in datasets but for better performance in undefined attacks, self-learning has been suggested by researchers.

- Deep belief network-Based Methods

The deep belief network is a deep neural network made up of stacked layers of Boltzmann Limited (RBM) machines designed to solve a problem related to slow learning of standard neural networks in training deep layered networks and sometimes with poor parameter selection get stuck [11]. A Boltzmann Limited machine is a useful algorithm for reducing size, partitioning, retransmission, shared filtering, learning features and title modelling [13].

Ad-hoc network intrusion detection got more attention recently and Tan et al. [13] proposed an intrusion detection based on DBN specific to the ad-hoc network by making use of the variety of available feature samples for the purpose of training their model in order to detect normal and abnormal traffic in the network. This DBN model is then used to detect interferences in the network traffic in which sequence is compared to the known abnormal behaviour characteristics of the network and if there are similarities between the new sequence and the already abnormal sequence then the model classifies as an attack or malicious acts [13].

Afterwards, Tan et al. [13] introduced an intrusion detection system based on DBN for Ad-hoc networks due to its behavioural characteristics. Their model contains 6 modules which helped their model achieve high accuracy up to 97.6% and in those modules, there is a data fetching module which is wireless monitoring nodes and a data integration module used to integrate useful data for redundancy removal. In order to train the model, a DBN training module is used and a DBN intrusion module is employed and then the results are given by the response module.

IEEE Computational Intelligence Society, International Neural Network Society, Institute of Electrical and Electronics Engineers, and B. C. [14] in their research proposed a DBN model which deals with large raw data by adjusting the different parameters such as the numbers of hidden layers. In adjusting parameters, they find that a four-layer DBN model is the best parameter that can achieve better performance using the KDDCup 99 dataset.

b. Review of Supervised Learning in intrusion Detection

- Deep neural network Methods

A deep Neural Network is a form of machine learning in which the system makes use of more than one layer of nodes to acquire high-level functions in input facts. The multi-layer feature of DNN helps to produce complex functions with a few parameters that help to extract the feature and learn to represent it. DNN is usually made of an input layer then follows the hidden layer and an output layer.

el Kamili and Institute of Electrical and Electronics Engineers [15] Introduced a DNN model for intrusion detection for flow-based anomaly as a solution to the network security problem. They built their model which contains an input layer as the starting layer and used three hidden layers and then completed their model with an output layer. They implemented their model using the NSL-KDD dataset to evaluate their model which has proven that the DNN model detects a zero-day attack.

Peng et al. [16] suggest a network access method, which makes use of a deep neural network to extract data features from network monitors and differentiate intrusion by using a neural BP network. As the result of their model in an experiment using a benchmark dataset KDD Cup99 has shown a good accuracy of 95.45% which compared to conventional machine learning has significant improvements and performs well.

In order to detect android malware, "Enhanced Reader" [17] proposed an android malware detection model using DNN known as HashTran-DNN. The main idea is to use space-saving hash functions to modify samples to reduce, if not eliminate, the impact of the opposing interference. They used an autoencoder to duplicate DNNs and recreate sample hash presentations. The figures below show the HasTran-Dan architecture and also the training and testing phases in their research (Fig. 1).

- Convolutional Neural Network Methods in intrusion detection

A convolutional neural network is a deep learning technique that can identify and then classify various specified features from images. CNN uses a mult-ilayer perceptron variant design which requires less or minimal pre-processing and this method is made of three main layers. In the first layer, there is the convolutional layer which extracts the various features and then comes the pooling layer that reduces the dimension of the output from the previous layer and in order to finalise the CNN process the last layer known as the fully connected layer, contains the weights and bias which helps adjust and connect all the neurons from past layers.

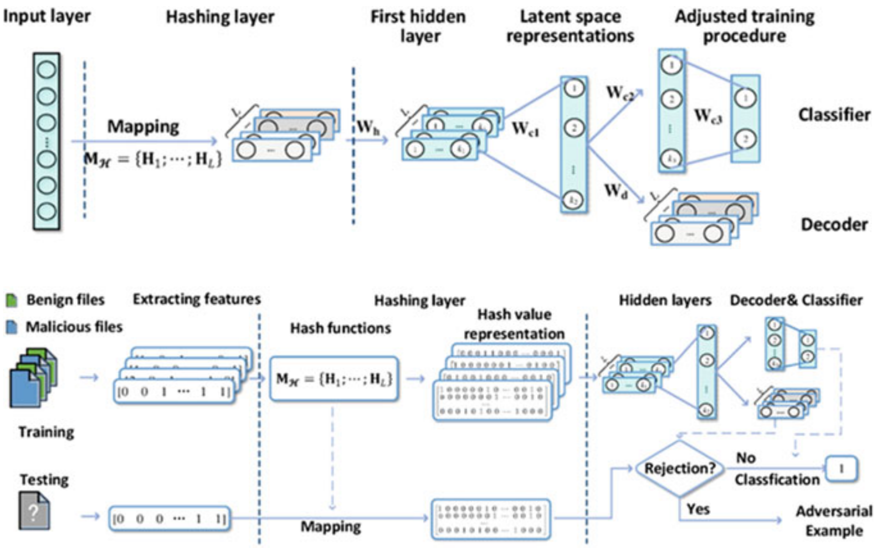


Fig. 1 **a** HasTran-Dan architecture proposed by "Enhanced Reader" [17]. **b** Training and testing phases in the HashTran-DNN proposed by "Enhanced Reader" [17]

The convolutional neural network has been employed in intrusion detection mechanisms which has shown much progress and enhanced their performance. Wang et al. [18] introduce a novel IDS that implements the CNN architecture, which consists of a data pre-processing module, and a training module to train their model with a testing module to help evaluate their system. Their model was built on the basis of the Linux platform and implemented using the NSL-KDD dataset. The results provided in the experiment show that their model can detect intrusion with high accuracy and elevated detection rate.

Wu and Guo [2] in the construction of their hierarchical convolutional neural network (LuNet), have considered that in network traffic data there is a presence of local and temporary features. LuNet is constructed with a succession of several convolutional layers in combination with recurrent sub-nets. The learning of data is done at each layer of the convolutional neural network and as the learning progresses, the data also gets detailed. The model has been implemented using two different datasets NSL-KDD and UNSW-NB15 which result in a very high detection rate with both datasets.

Deep learning being able to extract features automatically from a large dataset and also to share weight, Wu et al. [19] in their perspectives on improving the imbalanced traffic detection accuracy, have come up with a model of massive NIDS using the convolutional neural network. They suggested a method for setting the coefficients of the cost of each class's workload based on the number of training samples which resulted in better performances of the model. In the below figure they have given the architecture of their CNN of the model (Fig. 2).

Saxe and Berlin [20] proposed eXpose neural network which uses a convolutional neural network, in which the authentic short strings are taken as input and features are extracted in contribution to detect attack indicators. In this model, they used features which are extracted and classified using character-level embeddings. Since there was an issue with manual feature extraction, eXpose showed that it can overcome that issue in intrusion detection systems. The combination of supervised training with the embedded convolutions layers embeddings has allowed their model to benefit from implicit feature set extraction which is optimised for classifications.

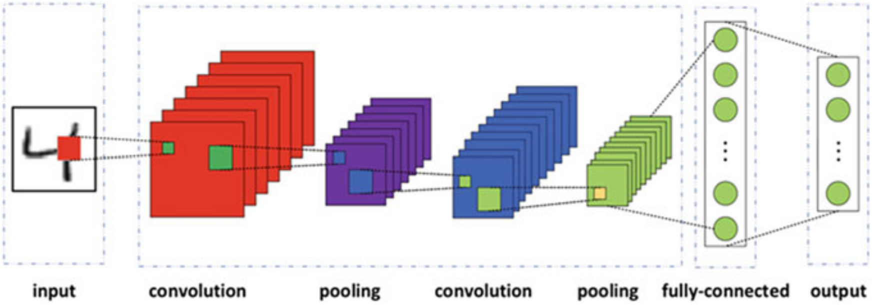


Fig. 2 The convolution neural network architecture proposed by Wu et al. [19]

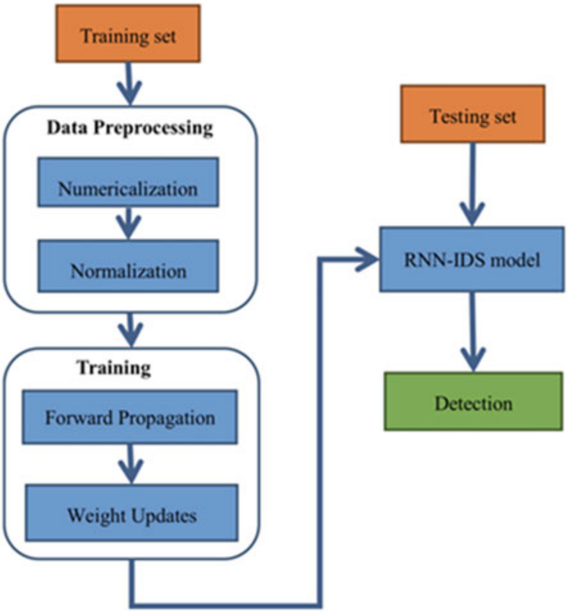
- Recurrent Neural Network-Based Methods

The ability of remembrance of previous layer information to impact the present layer input, made the Recurrent neural network to acquire more attention from various researchers in the construction intrusion detection system. So, when dealing with time-series information RNN is a good technique to use and its logic is like human cognition which is memory capability. With such functions and advantages, it's obvious that researchers have worked and proposed intrusion detection systems using RNN.

Yin et al. [21] came up with an intrusion detection system based on RNN in which multiclass and binary classification is used to evaluate their model. Their model profit from the remembering capability of the RNN to outperform compared to the CNN based model. The NSL-KDD dataset used for the experiment shows high accuracy achievement and that their model is best suited for class modelling and that its performance exceeds the standard machine learning methods. Figure 3 is the block diagram of their model.

Long short-term Memory (LSTM) is capable of recalling values during the processes and it is a type of recurrent neural network that has been used to develop IDS. In the classification and prediction of known and unknown attacks, LSTM is a suitable method and that is why Institute of Electrical and Electronics Engineers [22] proposed an intrusion detection system by applying LSTM-RNN. In this model, the design of a four-memory block network contains two cells each which results in high performance compared to previously proposed work.

Fig. 3 A flowchart of proposed RNN-IDS by Yin et al. [21]



ICT Platform Society [23] have used the LSTM in their proposed model for intrusion detection due to the advantage that is provided by the LSTM which is the resolution of the long-term dependency issue. The implementation of their model LSTM-RNN is done using KDD Cup99 dataset which showed great performance and compared to the model in Institute of Electrical and Electronics Engineers [22] this present model has high accuracy. At the end of the experiments with this model the size of the hidden layer was 80 and the learning rate was 0.01

Agarap [24] introduced a novel network classification system for finding attacks using a different GRU LSTM which uses the SoftMax function in the final layer (final output layer) of the model. As it is known that there are losses of information in the processes of the model the authors decided to use cross-entropy which helps calculate those losses. In order to improve their model, they made use of a linear support vector support (SVM) in replacement to the SoftMax function of the proposed GRU model and it resulted in high achievement compared to the original model and this is due to faster integration and better segmentation.

4 Comparisons and Analysis

The implementation of the various deep learning techniques is best achieved with two public datasets in the intrusion detection fields which are KDDCup 99 dataset and NSL-KDD.

- **KDDCup 99 dataset**

This dataset has been used before the other dataset was created and KDDCup 99 was generated from data originating from DARPA'98 IDS evaluation. The main issue in this dataset is the redundancy of training and testing data but that does not prevent its wide usage in the cybersecurity field. There are five categories of labels in the KDDCup 99 dataset, normal, DoS, which is an attack that prevents flooding the victim's network, making him unable to access his services, Probe, which is malicious surveillance to get user credentials for harming actions and the final two which are R2L remote to local refers to an attacker trying to get root privilege from offsite login to a local computer and the U2R user to root which a low privilege user trying to get administrative privileges. The Table 1 shows the various features and their descriptions.

- **NSL-KDD dataset**

As the KDD Cup 99 was having redundancy issues, the NSL-KDD was developed to solve those issues and has become one of the most used datasets in recent years. It isn't the handiest disposal of redundant information from the education and checking out but additionally sets the variety of data for each education and checking out that help to obtain greater accuracy in detection. NSL-KDD and KDD Cup 99 datasets

Table 1 KDD cup 99 features

No	Variable name	Type	No	Variable name	Type
1	Duration	Continuous	22	Is_guest_login	Discrete
2	Service	Discrete	23	count	Continuous
3	flag	Discrete	24	Srv_count	Continuous
4	Src_bytes	Discrete	25	Serror_rate	Continuous
5	Src_bytes	Continuous	26	Srv_serror_rate	Continuous
6	Dst_bytes	Continuous	27	Rerror	Continuous
7	land	Discrete	28	Srv_rerror	Continuous
8	Wrong_fragment	Continuous	29	Same_srv_rate	Continuous
9	urgent	Continuous	30	Diff_srv_rate	Continuous
10	hot	Continuous	31	Srv_diff_host_rate	Continuous
11	Num_failed_logins	Continuous	32	Dst_host_count	Continuous
12	Logged_in	Discrete	33	Dst_host_srv_coun	Continuous
13	Num_conpromised	Continuous	34	Dst_host_diff_srv_rate	Continuous
14	Root_shell	Continuous	35	Dst_host_diff_srv_rate	Continuous
15	Su_attempted	Continuous	36	Dst_host_same_src_port_rate	Continuous
16	Num_root	Continuous	37	Dst_host_srv_diff_host_rate	Continuous
17	Num_file_creations	Continuous	38	Dst_host_serror_rate	Continuous
18	Num_shells	Continuous	39	Dst_host_srv_serror_rate	Continuous
19	Num_access_files	Continuous	40	Dst_host_rerror_rate	Continuous
20	Num_outbound_cmd	Continuous	41	Dst_host_srv_rerror_rate	Continuous
21	Is_host_login	Continuous	42	Normal or attack	Discrete

are comparable in shape, with 4 assault sorts as cited before but the former is divided into KDDTest+ and KDDTrain+ which are shown in Table 2.

- **Evaluation metrics**

In the process of evaluating the performance of the deep learning technique and making analysis, various evaluation metrics are being used and the most used metrics are accuracy, precision, memory or recall, and F1-score. When the ACC displays a fraction of the predetermined amount of data in all data, the precision calculates the fraction of the predetermined for real attack prediction, recall indicates the truth

Table 2 NSL-KDD training and test data

Class	KDDTrain+	KDDTest+
DoS	45,927	74,588
Probe	11,656	2421
R2L	665	2754
U2R	52	200

positive predictions and the F1-score measures precision and recall and represents the balance of performance in both accuracy and memory.

5 Performance Comparison and Analysis of Various Deep Learning Techniques

As seen in section three above, various deep learning techniques have been used in construction detection systems which reveals the performance of each technique that has been evaluated using different metrics. Table 3 is a summary of the performances of the deep learning techniques evaluated using accuracy, precision, false positive rate and F1-score metrics. Though there are some unavailable metrics data, Table 3 still allows us to make a rough comparison amongst the different learning techniques.

We can note that the performance between different stages of attack detection methods varies. From Table 3, DBN, LSTM, CNN, and AE are achieving the adoption process through a downward spiral. At the same time, the hybrid methods are not compatible, because their functionality is closely related to the ensemble classifiers. DBN is the best in overall performance, because of its multi-layer natural properties in dealing with unlabelled data. LSTM can also gain higher overall performance than CNN by using temporary equipment for more accurate modelling.

We notice that RBMs and AEs are both widely used for intrusion detection systems due to the ability of both methods such as the ability to pretrain unlabelled data and adjust with less labelled data. In table three, we have seen the various performances of the different techniques of deep learning that the best performance has been achieved with the KDD Cup 99 dataset, i.e., 99.97% obtained by Sara et al. [22] with less data employed and with the NSL-KDD dataset provide lesser performance than the KDD Cup99 Niyaz et al. [25], therefore just show that NSL-KDD dataset is much realistic with less redundancy than the KDD Cup 99.

As observed in above section III, we can notice that the modified AEs perform better than the standard AEs and this is because with standard AEs there is a high risk of important information losses during compression which is not the case with improved AEs. The improved AEs has the ability to capture important information including additional design much more clearly and better than the previous AEs. Similarly, LSTM and GRU methods with their features in gate architecture and memory cells surpass RNN-based methods. In fact, such ingenious designs offer the opportunity to preserve long-term knowledge, thus better modelling for long-term relationships.

The remembrance functionality of the RNN keeps remembering the last moments by using the output of the previous layer as the input of the present layer, this functionality enhances the classification accuracy.

Table 3 Summary of the performances of the different deep learning techniques with the various datasets

Authors	DL technique	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
Xu et al. [6]	AE	CTU-UNB	98.40	98.44	98.40	0.9841
Shone et al. [3]	AE	KDD CUP'99	97.85	99.99	97.85	0.9747
Shone et al. [7]	AE	NSL-KDD	85.42	100	85.42	0.8408
Niyaz et al. [25]	Sparse AE	NSL-KDD	98.30	–	–	0.990
IEEE Staff [10]	AE	10% KDDCup 99	94.71	94.53	94.42	–
Morabito et al.[12]	DBN	NS2 simulation	90.27	96.4	–	–
Tan et al. [13]	DBN	KDDCup 99	97.60	–	–	–
IEEE Computational Intelligence Society, International Neural Network Society, Institute of Electrical and Electronics Engineers, and B. C. [14]	DBN	Simulation dataset	96.60	–	–	–
el Kamili and Institute of Electrical and Electronics Engineers [15]	DNN	NSL-KDD	74.67	83	75	0.74
Tang et al.	DNN	NSL-KDD	91.70	83.00	–	–
Peng et al. [16]	DNN	KDDCup 99	95.45	–	–	–
Han et al. [17]	DNN	Android malware	91.71	–	–	–
Vinayakumar et al. [7]	DNN	KDDCup 99	93.00	99.00	–	–
Wu and Guo [2]	CNN	NSL-KDD	85.35	97.43	–	–
Wu et al. [19]	CNN	NSL-KDD	80.10	–	–	–
Berlin and Saxe [20]	CNN	TensorFlow	92.00	–	–	–
Wang and Yang	CNN	KDDCup 99	95.36	95.55	–	0.930
Yin et al. [21]	RNN	NSL-KDD	83.28	–	–	–
Institute of Electrical and Electronics Engineers [22]	RNN-LSTM	KDDCup 99	99.97	99.5	99.5	–
ICT Platform Society [23]	RNN-LSTM	KDDCup 99	96.93	98.80	–	–
Agarap [24]	RNN-GRU	TensorFlow	84.15	–	–	–

6 Summary

Deep learning to process data makes use of a succession of layers which contribute to the promising results achieved by the unsupervised feature learning and pattern recognition. The improvement in performance of the intrusion detection using deep learning methods shows that deep learning techniques are important to network security in attack detection. Therefore, we made a classification of recent applications of deep learning techniques and their results in this paper.

There has been fundamental progress during the last few years in the studies concerning the application deeply and getting to know techniques in attack detection and features have shown super performances. But we can deny that there are still some limitations to those techniques. One of the major issues is the challenge to adapt deep learning methods like real-time classifiers of attack detection. Another problem is that in experiments that are more data involved, the results of the separation will be better, but many attack detection problems are lacking sufficient data. From the above analysis, we believe that this all-encompassing view is to the benefit of those who have ideas to improve the effectiveness of accurate detection.

References

1. Wu Y, Wei D, Feng J (2020) Network attacks detection methods based on deep learning techniques: a survey. Security and communication networks, vol 2020. Hindawi Limited. https://doi.org/10.1155/2020/8872923
2. Wu P, Guo H (2019) LuNet: a deep neural network for network intrusion detection. http://arxiv.org/abs/1909.10031
3. Shone N, Ngoc TN, Phai VD, Shi Q (2018) A deep learning approach to network intrusion detection. IEEE Trans Emerg Topics Comput Intell 2(1):41–50. https://doi.org/10.1109/TETCI.2017.2772792
4. Liao HJ, Richard Lin CH, Lin YC, Tung KY (2013) Intrusion detection system: a comprehensive review. J Netw Comput Appl 36(1):16–24. https://doi.org/10.1016/J.JNCA.2012.09.004
5. LeCun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521(7553):436–444. https://doi.org/10.1038/nature14539
6. Xu X, Chen Y, Zhang X, Liu Q, Liu X, Qi L (2021) A blockchain-based computation offloading method for edge computing in 5G networks. Softw Pract Experience 51(10):2015–2032. https://doi.org/10.1002/spe.2749
7. Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
8. Donalek C (2011) Supervised and unsupervised learning
9. Yu Y, Long J, Cai Z (2017) Network intrusion detection through stacking dilated convolutional autoencoders. Secur Commun Netw 2017. https://doi.org/10.1155/2017/4184196
10. IEEE Staff (2018) 2018 20th International conference on advanced communication technology (ICACT). IEEE
11. Al-jabery KK, Obafemi-Ajayi T, Olbricht GR, Wunsch II DC (2020) Selected approaches to supervised learning. Comput Learn Approaches Data Analyt Biomed Appl 101–123. https://doi.org/10.1016/B978-0-12-814482-4.00004-8

12. Morabito FC, Campolo M, Ieracitano C, Mammone N (2019) Deep learning approaches to electrophysiological multivariate time-series analysis. Artif Intell Age Neural Netw Brain Comput 219–243. https://doi.org/10.1016/B978-0-12-815480-9.00011-6
13. Tan Q-S, Huang W, Li Q An intrusion detection method based on DBN in ad hoc networks. www.worldscientific.com
14. IEEE Computational Intelligence Society, International Neural Network Society, Institute of Electrical and Electronics Engineers, and B. C. (2016) IEEE World Congress on Computational Intelligence, Vancouver, 2016 International joint conference on neural networks (IJCNN), 24–29 July 2016, Vancouver, Canada
15. el Kamili M and Institute of Electrical and Electronics Engineers (2016) Proceedings, 2016 international conference on wireless networks and mobile communications (WINCOM), October 26–29, 2016, Fez, Morocco
16. Peng W, Kong X, Peng G, Li X, Wang Z (2019) Network intrusion detection based on deep learning. In Proceedings-2019 international conference on communications, information system, and computer engineering, CISCE 2019, Jul. 2019, pp 431–435. https://doi.org/10.1109/CISCE.2019.00102
17. "Enhanced Reader"
18. Wang H, Cao Z, Hong B (2020) A network intrusion detection system based on convolutional neural network. J Intell Fuzzy Syst 38(6):7623–7637. https://doi.org/10.3233/JIFS-179833
19. Wu K, Chen Z, Li W (2018) A novel intrusion detection model for a massive network using convolutional neural networks. IEEE Access 6:50850–50859. https://doi.org/10.1109/ACCESS.2018.2868993
20. Saxe J, Berlin K (2017) eXpose: a character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys. http://arxiv.org/abs/1702.08568
21. Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5:21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
22. Institute of Electrical and Electronics Engineers (2018) SoutheastCon 2018. St. Petersburg, FL., Apr 19th-Apr 22nd, 2018
23. ICT Platform Society, Han'guk Kwahak Kisul Chŏngbo Yŏn'guwŏn, Institution of Creative Research Professionals, Institute of Electrical and Electronics Engineers. Kwangju Section, and Institute of Electrical and Electronics Engineers, 2016 International conference on platform technology and service (PlatCon): proceedings, 15–17 February 2016, Jeju, Korea
24. Agarap AFM (2018) A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data. In ACM international conference proceeding series, pp 26–30. https://doi.org/10.1145/3195106.3195117
25. Niyaz Q, Sun W, Javaid AY, Alam M (2015) A deep learning approach for network intrusion detection system. https://doi.org/10.4108/eai.3-12-2015.2262516