НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2023 Том 23 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2023 Vol. 23 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2023-23-2-352-363

A survey of network intrusion detection systems based on deep learning approaches

Duaa Wahab Al-Safaar[1]✉, Wathiq Laftah Al-Yaseen[2]

[1] College of Science for Women, University of Babylon, Babylon, 51002, Iraq
[2] Karbala Technical Institute, Karbala, 56001, Iraq
[2] Al-Furat Al-Awsat Technical University, Karbala, 56001, Iraq

[1] duaa.raheem.gsci6@student.uobabylon.edu.iq✉, https://orcid.org/0000-0002-2995-2342
[2] wathiq@atu.edu.iq, https://orcid.org/0000-0002-2155-2993

Abstract

Currently, most IT organizations are inclined towards a cloud computing environment because of its distributed and scalable nature. However, its flexible and open architecture is receiving lots of attention from potential intruders for cyber threats. Here, Intrusion Detection System (IDS) plays a significant role in monitoring malicious activities in cloud-based systems. The state of the art of this paper is to systematically review the existing methods for detecting intrusions based upon various techniques, such as data mining, machine learning, and deep learning methods. Recently, deep learning techniques have gained momentum in the intrusion detection domain, and several IDS approaches are provided in the literature using various deep learning techniques to deal with privacy concerns and security threats. For this purpose, the article focuses on the deep IDS approaches and investigates how deep learning networks are employed by different approaches in various steps of the intrusion detection process to achieve better results. Then, it provided a comparison of the deep learning approaches and the shallow machine learning methods. Also, it describes datasets that are most used in IDS.

Keywords

cloud computing, intrusion detection system, machine learning, deep learning

For citation: Al-Safaar D.W., Al-Yaseen W.L. A survey of network intrusion detection systems based on deep learning approaches. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 2, pp. 352–363. doi: 10.17586/2226-1494-2023-23-2-352-363

УДК 004.056.5

Обзор систем обнаружения сетевых вторжений, основанных на подходах глубокого обучения

Дуа Вахаб Аль-Сафар[1]✉, Ватик Лафтах Аль-Ясин[2]

[1] Вавилонский университет, Кербела, 51002, Ирак
[2] Технический институт Кербелы, Кербела, 56001, Ирак
[2] Технический университет Аль-Фурат Аль-Авсат, Кербела, 56001, Ирак

[1] duaa.raheem.gsci6@student.uobabylon.edu.iq✉, https://orcid.org/0000-0002-2995-2342
[2] wathiq@atu.edu.iq, https://orcid.org/0000-0002-2155-2993

Аннотация

В настоящее время большинство ИТ-организаций отдают предпочтение среде облачных вычислений, которая имеет распределенный и масштабируемый характер. При этом гибкая и открытая архитектура среды облачных вычислений привлекает большое внимание потенциальных злоумышленников из-за киберугроз. В данном случае система обнаружения вторжений (Intrusion Detection System, IDS) играет важную роль в отслеживании вредоносных действий в облачных системах. В работе представлен системный обзор существующих IDS, основанных на различных методах, таких как интеллектуальный анализ данных, машинное обучение и методы глубокого обучения. В последнее время методы глубокого обучения широко распространены в области

обнаружения вторжений при решении проблем конфиденциальности и угроз безопасности. В связи с этим важно исследовать подходы к исследованию глубокого обучения, применяемых на разных этапах процесса обнаружения вторжений. Выполнено сравнение подходов глубокого обучения и поверхностных методов машинного обучения. Приведено описание наборов данных, наиболее часто используемых в системах обнаружения вторжений.

Ключевые слова
облачные вычисления, система обнаружения вторжений, машинное обучение, глубокое обучение

Ссылка для цитирования: Аль-Сафар Д.В., Аль-Ясин В.Л. Обзор систем обнаружения сетевых вторжений, основанных на подходах глубокого обучения // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 2. С. 352–363 (на англ. яз.). doi: 10.17586/2226-1494-2023-23-2-352-363

Introduction

Cloud computing is a watershed point in technology innovation for quick data processing. When a new computing system is introduced, academicians and researchers grow concerned about its security. The ability to protect information processing has become critical to the systems success. Cloud computing enables quick and location-independent data processing. Because of the location-independent processing, trust is one of the key difficulties that Cloud customers face when using its resources. As a result, Cloud security is critical for the successful deployment of its services. In comparison to an in-built security mechanism, a third-party security solution is not appealing due to security concerns. This is where the Intrusion Detection System (IDS) comes into play [1]. If it detects any unusual patterns that might point to an attack on the network, IDS notifies the network (or system) administrator automatically. An IDS is a great solution for securing cloud computing since it can detect known/unknown (inside/outside) assaults. In order to distinguish attacks more accurately, an IDS employs a variety of ways [2]. Deep Learning (DL) models are becoming more and more significant, and they have emerged as a promising field of research. Multiple deep networks can be employed in DL methodologies to increase the performance of IDSs. In terms of accuracy and generalization, DL models beat shallow Machine Learning (ML) models. In addition, DL methods don't need to know how to build features or how to work in a certain field. This gives them a big advantage over shallow machine-learning models [3].

Intrusion Detection System

The terms "intrusion detection system", or IDS, are a combination of the two terms. Unauthorized access to data in a computer or network system that violates its availability, confidentiality, or security is referred to as intrusion [4], whereas a detection system is a security tool for spotting this sort of violent conduct. Therefore, IDSs are hardware or software systems that monitor and control the operation display network or computer system occurrences and analyze them from a security point of view. As network threats rise, IDS is now a crucial complement to cybersecurity [5].

IDS Classification

It is possible to categorize IDSs using several methodologies illustrated in Fig. 1 [6]. It can be classified based on attack type for Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS). NIDS are positioned strategically throughout the network to watch traffic. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. In contrast, HIDS operates on different hosts or the network devices and only monitors incoming and outgoing packets from the device alerting the user or supervisor if a strange activity is discovered.

There are several IDS that look for specific signatures of known risks in order to find threats, the same as how antivirus programs normally identify threats and guard against malware, a process known as Signature-based Detection (SD). A pattern or string that is associated with a known threat or attack is called a signature. SD is sometimes referred to as knowledge-based detection or misuse detection because of the fact that it makes use of the information gathered by particular threats and system flaws.

There are IDSs that check for anomalies by comparing traffic patterns to a baseline and detecting them. An illustration of this kind of IDS is anomaly-based IDS which will track network activity and evaluate it in comparison to a predetermined standard. The baseline can observe often network threats by comparing the present anomalous behavior with what is thought to be usual. It will notify the supervisor or user when connectivity is observed that is anomalous, or completely different, from the baseline. The baseline will define an intrusion when the analyzed activities in computer systems display a huge variance from the usual case profile constructed on long-term regular activities [6].

IDSs are divided into active and passive ones when they are categorized according to how they behaved following the attack. The benefit of proactive IDS is that it can immediately take corrective action in the event of an attack. An IDS that just monitors and analyzes network traffic activity and notifies an operator of potential threats

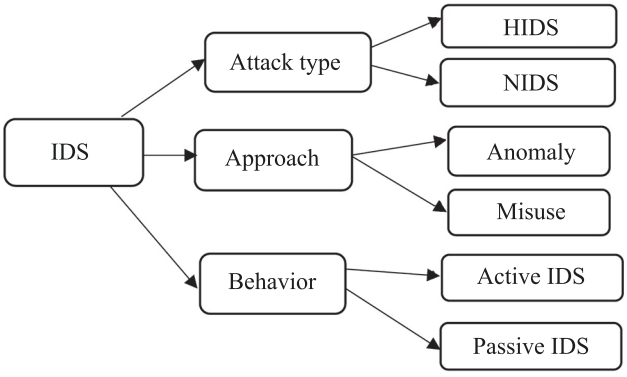

Fig. 1. The IDS classification types

and flaws is known as a passive IDS. A passive IDS cannot, by itself, carry out any defensive or remedial actions [6].

Deep Learning Models Based IDS

It's important to develop efficient methods for detecting violent acts, fending them off, and maintaining network security. Furthermore, various violence types typically need to be handled in various ways. Thus, the primary problem in the field of network security is how to recognize several forms of malicious activities, particularly ones which haven't been seen previously. Across recent years, researchers have categorized network violent acts using a variety of ML techniques without having any previous knowledge of their specific properties. Furthermore, owing to the constraints on model accuracy, existing ML techniques cannot offer distinguishing feature descriptors to describe the difficulty of detection accuracy. Lately, DL techniques, named for their overall design of deep tiers to address challenging troubles, have achieved a significant advancement in ML by modeling the human brain with neural network structure [7].

One of the hot topics in current academic study is the use of DL for network intrusion detection. The advancement of hardware computer power and the quick increase in data size has encouraged the development of DL which has substantially increased its applicability and popularity [8]. DL is a ML technology created to enable artificial intelligence to enhance computer systems through experience and data. To describe data learning, DL employs numerous nonlinear feature transformations or processing tiers created by multilayer perceptual processes [8]. Since 2015, DL research for network security has increasingly come into focus, garnering significant interest from academics. The IDS is depicted in Fig. 2, and the researchers concentrated on DL techniques for its design. It is notable that only 20 % of recommended solutions are based on ML models, while 60 % of proposed ways are totally dependent on DL techniques, and 20 % of solutions use a hybrid strategy that combines ML and DL-based techniques. DL enhances detection effectiveness and lowers false positives when compared with standard ML which is currently employed mostly in the two core network security domains of malware detection and network intrusion detection [5]. Additionally, DL techniques eliminate the need for feature engineering and have the capacity to automatically recognize attack features, aiding in the

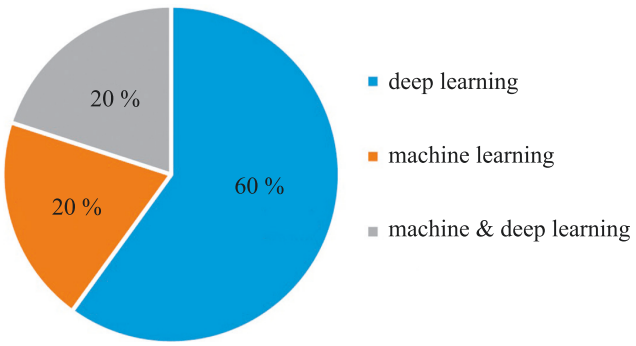

Fig. 2. Distribution of techniques

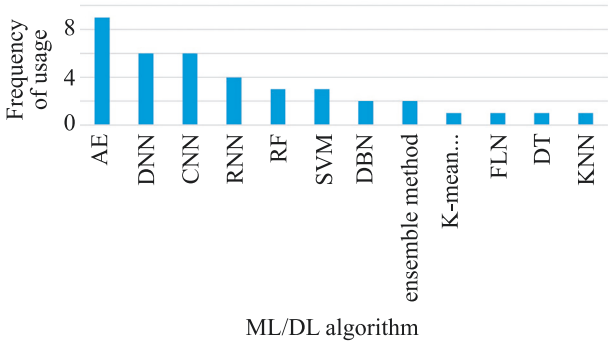

Fig. 3. How widely deep learning and machine learning methods are employed

detection of potential security flaws. Moreover, Fig. 3 displays how frequently ML or DL-based techniques are used by researchers to create effective IDS solutions. The four most often employed techniques, all of which are DL in type, are noticed to be Auto Encoder (AE), Deep Neural Network (DNN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN), in that order. Following that, ML-based methods like Random Forest (RF) and Support Vector Machines (SVM) are included in the ranking and are primarily utilized in combination designs to support and enhance DL-based techniques. Additionally, less often used ML-based techniques include Decision Tree (DT), K-Nearest Neighbor (KNN), and Fast Learning Network (FLN) [5].

Three main categories are used to classify deep networks: unsupervised (e.g., AE, Deep Belief Network (DBN), and Generative Adversarial Network (GAN)), supervised (e.g., DNN, CNN, and RNN), and other hybrid techniques; we display the classification information to Security and Communication Networks in Fig. 4 [9]. Various DL techniques could offer multiple benefits for attack detection techniques. Because of the large amount of data offered by manually labeled samples, supervised learning-based algorithms frequently produce excellent accuracy. Unsupervised learning-based techniques typically perform poorly without enough information from labeled data. However, manually labeling takes a while, particularly for complicated attacks. Due to the intrinsic complexity of actual network attacks, there are circumstances that cannot be adequately characterized by a single label. Therefore, approaches based on unsupervised learning could function effectively without being aware of attacks beforehand, which is a clear advantage. Hybrid approaches use fewer training samples while maintaining excellent performance, making them suited for dealing with a variety of assault scenarios. However, its widespread use is limited by its typically intricate design and lengthy processing time.

Unsupervised Deep Learning

Auto Encoder

Two symmetrical elements exist in an AE: an encoder and a decoder. The encoder takes the raw data and derives features, whereas the decoder uses those characteristics to reconstruct the data. Slowly reducing the discrepancy between the decoder output and the encoder input occurs

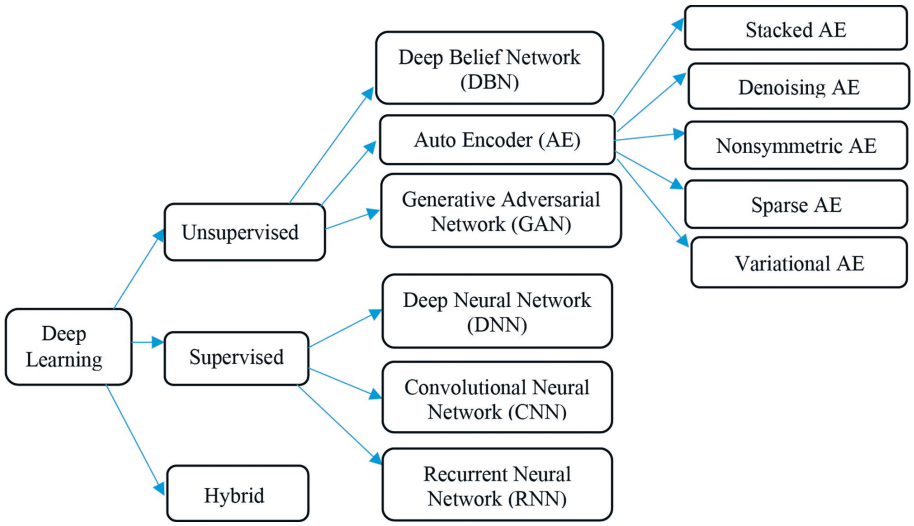

Fig. 4. Classification of the available deep learning intrusion detection techniques

throughout training. The encoder factors reflect the data core if the decoder is able to recreate the data using the extracted features. It's worth noting that this entire procedure does not necessitate the use of supervised data. Denoising AEs [10, 11] and sparse AEs [12] are two well-known AE types. A design pattern is shown in Fig. 5, where $\mathbf{h}(\mathbf{x})$ represents the hidden encoder vector calculated from input vector $\mathbf{x}$, and $\tilde{\mathbf{x}}$ is the decoder (or reconstruction) vector of the output layer. $\mathbf{W}$ and $\tilde{\mathbf{W}}$ are the weight matrix of the encoder and decoder, respectively.

Yan and Han [13] recommended using the Stacked Sparse Autoencoder (SSAE), a DL approach, to extract high-level feature representations of intrusive behavior information. For the first time, SSAE incorporates the original categorization characteristics to automatically learn deep sparse features. After that, the low-dimensional sparse features are used to create a variety of simple classifiers. SSAE is compared to a variety of other academically presented feature extraction methods. The experimental findings in binary and multiclass classification support the following conclusions: 1) SSAE learned high-dimensional sparse features are more discriminatory for incursion behaviors than previous techniques, and 2) using high-dimensional sparse features accelerates the classification process of basic classifiers.

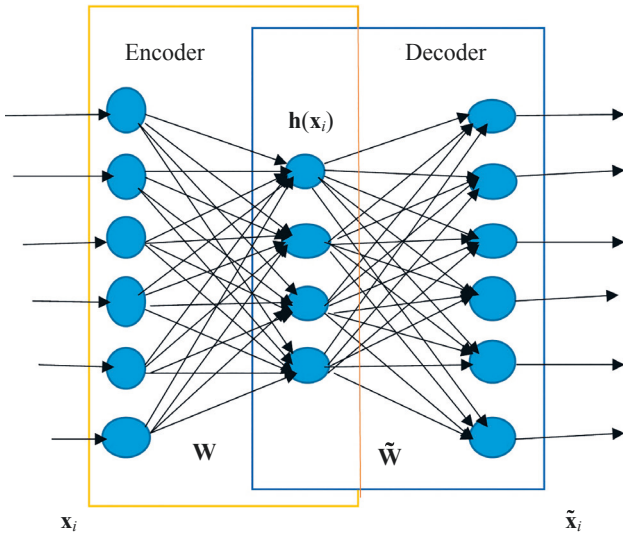

Fig. 5. The structure of an Auto Encoder

Farahnakian et al. [14] utilize deep stacked AE to focus on important and informative feature representations, thus constructing classification models to detect abnormal behaviors. Specifically, their proposed network consists of 4 AEs in sequential order that will be trained in a greedy layer wise fashion. Experimental results on KDD Cup 99 dataset show it could achieve high accuracy for abnormal detection, that is, 94.71 %.

A new deep-learning IDS developed by Shone and Nguyen Ngoc [15] addresses these difficulties. They provided a Nonsymmetric Deep AE (NDAE) for unsupervised feature learning. A DL classification model using stacked NDAEs is also presented. With the use of Tensor Flow and GPU assistance, they created and tested the proposed classifier on the KDD Cup 99 and NSL-KDD datasets, respectively, achieving promising results compared with others.

C. Zhang et al. [16] proposed approach is based on DL for IDS to address the issue to some extent. Used AE and the suggested method developed the network and discovered threats more quickly by using the encoder of the deep AE to reduce the less significant characteristics and extract crucial features without a decoder. The framework was evaluated by using NSL-KDD datasets for 5 classes, the accuracy rate is 79.74 %.

M. Al-Qatf et al. [17] suggested a successful DL strategy built on the IDS for Self-Taught Learning (STL). The Sparse AE (SAE) and SVM are combined in the suggested method to learn features and reduce dimensionality. It effectively increases the SVM attack prediction accuracy while reducing the training and testing times by a significant amount. The NSL-KDD dataset is used to validate the methodology for binary and multi-classification, KDDTrain+ 10-fold cross-validation must be employed to determine whether the model is effective for five-class categorization. The accuracy rate was 84.96 % and 80.48 % respectively.

Zhang et al. 2020 [18] presented a new network intrusion detection method based on AE and Long Short-term memory (LSTM) neural network. First, KDD Cup 99 data set is used and pre-processed. And an AE network model is constructed by superimposing multiple AE networks to map high-dimensional data to low-dimensional space. Then the optimized the cell structure LSTM model was used to extract features, train data and predict intrusion detection types. The experimental results show that compared with several classical methods, the accuracy of network intrusion detection is improved by 2 % on average, and the false alarm rates are lower.

Deep Brief Network (DBN)

DBN could be divided into two categories, that is, Restricted Boltzmann Machines (RBM) with several layers of unsupervised learning networks and Backpropagation Neural Network (BPNN or BP) with one such layer. Fig. 6 depicts a DBN made up of several RBM layers and a softmax classification algorithm. Unsupervised pretraining and supervised fine-tuning are two of the 2 steps of DBN training. Each RBM is initially pretrained using greed layer-wise pretraining. After that, the weight of the softmax layer is determined from the labeled data. DBNs are used in attack detection to extract features and classify such features [19, 20].

Gao et al. [21] focus on dealing with big raw data and implementing deep belief networks to construct such IDSs. In their paper, they try different DBN methods by adjusting parameters like the number of layers and hidden layers. They find that the best parameter settings for DBN is a four-layer DBN model which could achieve better performance than other ML methods on KDD Cup 99 dataset.

Gafarou O. Coli et al. [22] developed a deep learning-based model for detecting DDoS in IoT, taking into account its peculiarities. The proposed deep learning-based model was formulated using a deep Gaussian-Bernoulli restricted Boltzmann machine (DBM) because of its capability to learn high-level features from input following the unsupervised approach and its ability to manage real-time data that is common in the IoT network. Furthermore, the Softmax regression was used for classification. The accuracy of the proposed model on the network socket layer-knowledge discovery in databases was obtained as 93.52 %. The outcome of the study shows that the proposed DBM can efficiently detect DDoS attacks in IoT.

Generative Adversarial Network (GAN)

For the generator and the discriminator, a GAN model contains two separate subnetworks. Generating data that appear like the genuine thing is the purpose of the generator; however, the discriminator goal is to be able to recognize when something is fake. As a result, the generator and discriminator complement one another. GANs are a trendy study area right now, and they are being utilized to supplement data in the identification of attacks which helps to alleviate the issue of IDS dataset scarcity. GANs, on the other hand, are adversarial learning algorithms that can improve model detection accuracy by including adversarial samples in the training set.

Even though GAN is new in conception and hard in the training process, researchers successfully build several attack detection applications by regarding it as basic structure. For instance, Erpek et al. [23] propose a GAN-based approach to detect jamming attacks on wireless communications and defend it based on collected information of attacks. Specifically, their model consists of a transmitter, a receiver, and a jammer. A pretrained classifier is adopted by the transmitter to predict the current channel state and decide whether to send based on the latest sensing results, while the jammer collects the channel state and acknowledgments to construct a classifier which could predict next transmission and block it successfully. The jammer uses classification score to control the power under the average power constraint. Afterward, a GAN is designed to perform as a jammer, which can cut down collection time by adding synthetic samples.

Supervised Deep Learning

Deep Neural Network (DNN)

We represent a supplement of a feed-forward neural network. It consists of 3 types of tiers: the input tier, output tier, and hidden tier. Such multilayer feature brings the advantage to express complex functions with fewer parameters that makes DNN capable of facilitating tasks of feature extraction and representation learning. Fig. 7

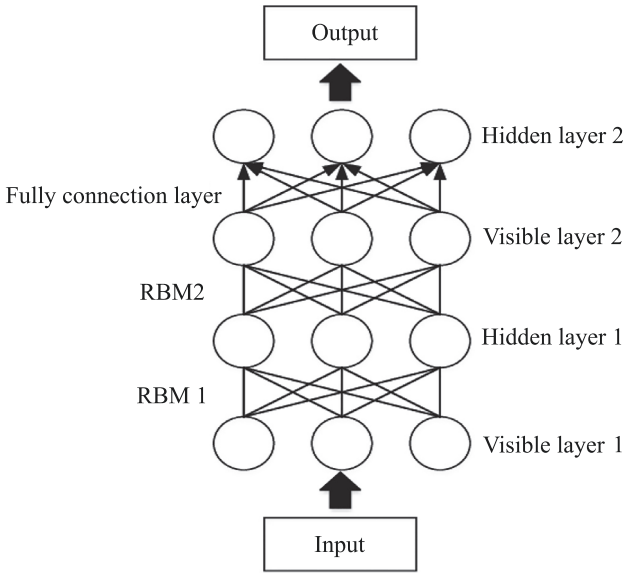

Fig. 6. The structure of the DBN

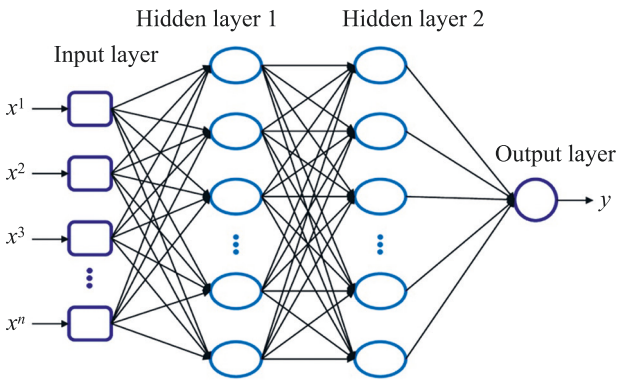

Fig. 7. The structure of the DNN

illustrates the structure of DNN, where x is an input layer, n is the number of input layer and y is the output layer.

To solve the problems of feature extraction and low detection accuracy in intrusion detection, an intrusion detection model SAAE-DNN, based on SAE, attention mechanism, and DNN, is proposed by Tang et al. [24]. The SAE represents data with a latent layer, and the attention mechanism enables the network to obtain the key features of intrusion detection. The trained SAAE encoder can not only automatically extract features, but also initialize the weights of DNN potential layers to improve the detection accuracy of DNN. They evaluate the performance of SAAE-DNN in binary classification and multi-classification on an NSL-KDD dataset. The SAAE-DNN model can detect normally and attack symmetrically, with an accuracy of 87.74 % and 82.14 % (binary-classification and multi-classification) which is higher than that of ML methods, such as RF and DT. The experimental results show that the model has a better performance than other comparison methods.

Convolutional Neural Network (CNN)

They have made tremendous progress in computer vision since CNNs are designed to mimic the Human Visual System. To retrieve features, convolutional and pooling layers are employed. In order to detect assaults using CNNs, the input data must be turned into matrices since CNNs only work with 2-dimensional (2D) data.

Saleem, Naseer, and other people wrote a paper about this in 2018 [25]. The focus of this article is to find out if DL algorithms can be used to make anomaly-based IDSs work better. CNNs, AEs, and RNNs are some of the different DNN topologies that were used in this study. A training set called NSLKDD was used to train these deep models.

They were then tested with NSLKDD test data sets, NSLKDD Test+ and NSLKDD Test21.

A multi-classification network intrusion detection model based on CNN is proposed by Liu and Zhang [26]. First, the data is preprocessed, the original one-dimensional network intrusion data is converted into two-dimensional data, and then the effective features are learned using optimized (CNNs), and, finally, the final test results are produced in conjunction with the Softmax classifier. In this paper, KDD Cup 99 and NSL-KDD standard network intrusion detection dataset were used to carry out the multi classification network intrusion detection experiment; the experimental results show that the multi classification network intrusion detection model proposed in this paper improves the accuracy and check rate, reduces the false positive rate, and also obtains better test results for the detection of unknown attacks.

Al-Emadi et al. [27] used DL techniques, namely, CNN and RNN to design an intelligent detection system which is able to detect different network intrusions. Additionally, we evaluate the performance of the proposed solution using different evaluation matrices, and we present a comparison between the results of our proposed solution to find the best model for the network IDS. We used the NSL-KDD dataset for the purpose of training and testing. Among the tested DL techniques, CNN found to have outperformed the other techniques with accuracy, F1 score, recall and precision of above 97 %.

Recurrent Neural Network (RNN)

RNNs are data-flow networks that are widely used in Natural Language Processing [28, 29]. RNN is proposed as a special category of neural network structures designed with a “memory” function to maintain previous content. However, there are still some problems in the structural design of RNN like gradient disappearance or gradient explosion which leads to failure to remember or model long-time dependence. Therefore, researchers develop LSTM and Gated Recurrent Unit (GRU) with gates design and memory cells which successfully keep long-time relationships unforgotten by passing through important components of information flow.

The authors of this research, T. Thilagam and R. Aruna [30] present an IDS for Optimized RC-NNs for the Ant Lion optimization approach (Recurrent Convolutional Neural Network). Conventional Neural Networks are combined with the LSTM. Thus, any assaults detected at the cloud network layer may be categorized effectively. IDS classification model is shown to be very accurate, resulting in an improved detection rate or error rate in the following experimentation findings. After making several adjustments to its original model, the modified RC-NN-IDS model improved classification accuracy by 94 % and reduced error rates by 0.0012. Additionally, performance metrics, such as true positive rate, true negative rate, and accuracy, are examined. The suggested method is compared to current techniques using the DARPA IDS assessment datasets and the CSE-CIC IDS2018 dataset.

In this article, Prabhakaran and Kulandasamy [31] merge LSTM, CNN, and SVM architectures in a SVM. An embedding layer known as the Word2Vec layer is used to detect semantic information in network data. Assault-class text incursions are given in the HSDL model. For cloud storage security, regular text is encrypted using the Advanced Encryption Standard (AES) method, and the ideal AES algorithm key with the quickest key breaking time is obtained using the Crossover-based Mine Blast optimization Approach. Two real-time intrusion detection benchmark datasets, NSL-KDD and UNSW-NB15, are used to evaluate and test the proposed HSDL system. It has the accuracy of 99.98 % for the NSL-KDD dataset, and correctness of 98.47 % for the UNSW-NB15 dataset, to propose this model. The recommended strategy has been shown to be effective and robust in experiments and security investigations.

Datasets in IDS

Many public datasets are popular to prove and compare efficiency and effectiveness among different attack detection methods. Among them, we list two famous benchmark datasets, that is, KDD Cup 99 and NSL-KDD, which are widely used in the academic research to evaluate the ability to detect attacks.

KDD Cup 99[1]

Currently, the KDD Cup 99 dataset is the most widely used IDS benchmark dataset. Its compilers mined

[1] KDD99 Dataset. 1999. Available online: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed: 16.10.2019).

Table 1. Number of training and testing examples in KDD Cup 99 Dataset

Category	Training examples	KDD, %	Testing examples	%
Normal	97,278	19.69	60,593	19.48
Dos	391,458	79.24	229,853	73.90
Probe	4107	0.83	4166	1.34
R2L	1126	0.23	16,189	5.20
U2R	52	0.01	228	0.07
Total	**494,021**	—	**311,029**	—

Table 2. Distribution of instance in NSL-KDD dataset for training and testing

Types of Attack	Number of Records	
	Training Dataset	Test Dataset
Normal	67,343	9711
Denial of service	45,927	7456
Probe	11,656	2421
Remote to local	995	2756
User to root	52	200
Total	**125,973**	**22,544**

DARPA1998 data for 41-dimensional characteristics. The labels in KDD Cup 99 are identical to the ones in DARPA1998.

Table 1 illustrates the number of training and testing examples in KDD Cup 99.

The training dataset contains 22 types of attacks in addition to those in the normal class, whereas the testing dataset contains only an additional 17 types of attacks that are not present in the training dataset. Furthermore, each instance in the dataset displays 41 continuous and discrete attributes (38 numerical and 3 symbolic) [32].

NSL-KDD[1]

NSL-KDD was created to fill the gap. Using the KDD Cup 99 as a reference, the recordings in the NSL-KDD were chosen. In Table 2 we illustrate the distribution of instance in NSL-KDD dataset for training and testing. As a result, NSL-KDD avoids the problem of categorization bias. Duplicate and superfluous records were also removed using the NSL-KDD and reducing the overall volume to a reasonable level.

Comparisons and Performance Analysis

In this section, concise overview of the different DL techniques and datasets are used for IDS in different references. In Table 3, we offer detailed statistics on attack detection results achieved by various methods listed in the previous section, where most of the listed DL methods are designed to perform network intrusion detection and malware detection. The comparison is based on the DL method used, the datasets, the full datasets, cross-validation, and the binary, multi-class classification. Additionally, among the number of measurements, we select accuracy for evaluation since most of the listed methods use this measurement for experiments. We must emphasize that there exist imbalances in performance comparisons since different authors adopt different datasets, measurements, and settings.

We observe that the improvement in the accuracy of detection is related to the techniques of DL used, the datasets, and the number of features. Essentially, it is interesting to point out that RBMs and AEs are popular in intrusion detection because we can pretrained the RBMs and AEs with unlabeled data and fine-tune with only a small number of labeled data. Accuracy values achieved by listed methods are the first evaluation index due to its completeness. We can observe that performance of AE-based methods is uneven; there most of the improved AE-based methods obviously perform better than traditional AE-based methods. This is due to the fact that the structure of AE might lose important information during the compression process. Meanwhile, improved AE could better capture important and informative parts of input data with additional designs. Similarly, LSTM-based and GRU-based methods outperform RNN-based methods, due to their features in the structure design of gates and memory cells. In fact, such intelligent designs bring the advantage of the capability of maintaining long-term information, thus better modeling long-time relationships. Additionally, we notice the combining supervised and unsupervised learning may provide better performance which has been proved by many trials.

[1] NSL-KDD99 Dataset. 2009. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed: 16.10.2019).

Table 3. Experiments evaluation of listed attack detection methods using different deep learning techniques

Reference	Technique	Dataset	Cross validation	Full training and testing datasets	Dataset size: training/testing	Binary classification	Multi classification	Accuracy
[13]	SSAE + SVM	NSL-KDD	✓	×	74,487 training dataset size 22,543 test samples	✓	×	99.35 %
[14]	DAE	KDD Cup 99	✓	×	Training records 494,021, testing records 311,029	✓	×	96.53 % – Binary-classification 94.71 % multi-classification
[15]	NDAE DBN S-NDAE	KDD Cup 99, NSL-KDD	✓	×	494,021 training records and 311,029, testing records for KDD Cup 99 full NSL-KDD	✓	×	KDD Cup 99 No. Training No.attacks DBN / S-NDAE 97.90 %/97.85 % 494,021/292,300 NSL-KDD 5-CLASS 80.58 %/85.42 % 125,973/18,794 NSL-KDD 13-CLASS 89.22 % 125,881/17,802
[16]	AE	Full NSL-KDD	×	✓	Full dataset	×	×	79.74 %
[17]	STL, (SAE + SVM)	NSL-KDD	✓	×	×	✓	×	84.96 % (class 2) 80.48 % (class 5)
[18]	AE + (LSTM)	KDD Cup 99	✓	×	Full dataset	✓	×	For 5 kinds of attack behavior was: 97.6 %, 96.8 %, 95.3 %, 94.8 % and 94.7 % respectively
[21]	DBN	KDD Cup 99	✓	×	×	×	×	93.49 %
[22]	Deep Gaussian-Bernoulli restricted Boltzmann machine (DBM)	NSL-KDD	✓	×	Holdout set validation method was used to build the final model with the training dataset for training (70 %), validation (10 %), and testing (20 %)	✓	×	93.52 % in 2-classes 91.69 % in 5-classes
[24]	SAAE-DNN	NSL-KDD dataset	✓	×	KDDTrain+ as the training set and KDDTest+ and KDDTest-21 as the testing sets, 5,346, 4,307, and 1,816, respectively	✓	×	87.74 % binary-classification 82.14 % multi-classification
[25]	CNN, AEs, and RNN, LSTM	NSL-KDD	✓	×	NSLKDD Train20p and NSLKDD Train+ provide 25,192 and 125,973 training records NSLKDD Test+ and Test21 assess trained models on unknown data. 22,543, 11,850 data samples	✓	×	LSTM has the best accuracy with 89 and 83 % NSL-KDD Test+ and Test21

Table 3. Continuation

Reference	Technique	Dataset	Cross validation	Full training and testing datasets	Dataset size: training/testing	Binary classification	Multi classification	Accuracy
[26]	CNN	KDD Cup 99 and NSL-KDD	✓	×	Training and testing employ 10 % of the KDD Cup 99 dataset. 75 % of the training data should be used as the training set. Complete NSL-KDD	✓	×	98.02 % KDD Cup 99 dataset 97.09 % In NSL-KDD
[27]	CNN RNN - LSTM RNN - GRU	NSL-KDD	✓	×	85 % used for the training process and 15 % for validation and testing	✓	×	CNN 97.01 % RNN-LSTM 81.60 % RNN-GRU 50.25 %
[30]	RC-NN (LSTM)	DARPA, CSE-CIC-IDS2018	✓	✓	×	✓	×	94.01 % for DARPA 94.28 % for CSE-CIC-IDS2018
[31]	LSTM + CNN + SVM	NSL-KDD and UNSW-NB15	✓	×	In NSL-KDD no. of Training 125,973 no. of Testing 22,544 The UNSW-NB15 dataset is divided into two subsets where 70 % of the data is used for training, 30 % of data is used for testing	✓	×	NSL-KDD 99.98 % UNSW-NB15 98.47 %

Conclusion

It is vital that cloud security is to be protected by IDSs. Various AI approaches are used in IDSs in order to improve their performance and efficacy in the face of emerging security threats. To enhance feature extraction and classification in the IDS methods, researchers have focused on deep learning techniques. There have been a number of deep learning-based IDS solutions suggested in the literature in recent years; this work aims to give an in-depth assessment and categorization of them. Deep learning models are playing an increasingly important role and have become an outstanding direction of study. Deep learning approaches include multiple deep networks which can be used to improve the performance of IDSs. Compared with shallow machine learning models, deep learning models own stronger fitting and generalization abilities. In addition, deep learning approaches are independent of feature engineering and domain knowledge which takes an outstanding advantage over shallow machine learning models. As a result, it initially gives background information, illustrates the various types of deep learning networks used in the investigated IDS techniques. It also includes descriptions of the major datasets used to assess and analyze the IDS schemes. We provide the overview of the different deep learning techniques and datasets used for IDS in different references. We offer detailed statistics on attack detection results achieved by various methods of deep learning summarized in Table 3.

References

1. Deshpande P., Sharma S.C., Peddoju S.K., Junaid S. HIDS: A host based intrusion detection system for cloud computing environment. *International Journal of System Assurance Engineering and Management*, 2018, vol. 9, no. 3, pp. 567–576. https://doi.org/10.1007/s13198-014-0277-7
2. Shamshirband S., Fathi M., Chronopoulos A.T., Montieri A., Palumbo F., Pescapè A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*, 2020, vol. 55, pp. 102582. https://doi.org/10.1016/j.jisa.2020.102582
3. Aldweesha A., Derhabb A., Emamc A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A Survey, taxonomy, and open issues. *Knowledge-Based Systems*, 2020, vol. 189, pp. 105124. https://doi.org/10.1016/j.knosys.2019.105124
4. AbdAllah E.G., Zulkernine M., Hassanein H.S. Preventing unauthorized access in information centric networking. *Security and Privacy*, 2018, vol. 1, no. 4, pp. e33. https://doi.org/10.1002/spy2.33
5. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 2021, vol. 32, no. 1, pp. e4150. https://doi.org/10.1002/ett.4150
6. Tun H., Lupin S., Linn H.H., Lin K.N.Z. Selection the perimeter protection equipment in security systems. *Proc. of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2018, pp. 1504–1508. https://doi.org/10.1109/eiconrus.2018.831738
7. Saxena A., Mueller C. Intelligent intrusion detection in computer networks using swarm intelligence. *International Journal of Computer Applications*, 2018, vol. 179, no. 16, pp. 1–9. https://doi.org/10.5120/ijca2018916224
8. Liu G., Zhang J. CNID: Research of network intrusion detection based on convolutional neural network. *Discrete Dynamics in Nature and Society*, 2020, vol. 2020, pp. 1–11. https://doi.org/10.1155/2020/4705982
9. Wu Y., Wei D., Feng J. Network attacks detection methods based on deep learning techniques: A survey. *Security and Communication Networks*, 2020, vol. 2020, pp. 1–17. https://doi.org/10.1155/2020/8872923
10. Vincent P., Larochelle H., Bengio Y., Manzagol P.-A. Extracting and composing robust features with Denoising autoencoders. *Proceedings of the 25th International Conference on Machine learning (ICML)*, pp. 1096–1103. https://doi.org/10.1145/1390156.1390294
11. Vincent P., Larochelle H., Lajoie I., Bengio Y., Manzagol P.A. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. *Journal of Machine Learning Research*, 2010, vol. 11, pp. 3371–3408.
12. Deng J., Zhang Z., Marchi E., Schuller B. Sparse autoencoder-based feature transfer learning for speech emotion recognition. *Proc. of the 2013 Humaine Association Conference on Affective Computing and*

Литература

1. Deshpande P., Sharma S.C., Peddoju S.K., Junaid S. HIDS: A host based intrusion detection system for cloud computing environment // International Journal of System Assurance Engineering and Management. 2018. V. 9. N 3. P. 567–576. https://doi.org/10.1007/s13198-014-0277-7
2. Shamshirband S., Fathi M., Chronopoulos A.T., Montieri A., Palumbo F., Pescapè A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues // Journal of Information Security and Applications. 2020. V. 55. P. 102582. https://doi.org/10.1016/j.jisa.2020.102582
3. Aldweesha A., Derhabb A., Emamc A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A Survey, taxonomy, and open issues // Knowledge-Based Systems. 2020. V. 189. P. 105124. https://doi.org/10.1016/j.knosys.2019.105124
4. AbdAllah E.G., Zulkernine M., Hassanein H.S. Preventing unauthorized access in information centric networking // Security and Privacy. 2018. V. 1. N 4. P. e33. https://doi.org/10.1002/spy2.33
5. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches // Transactions on Emerging Telecommunications Technologies. 2021. V. 32. N 1. P. e4150. https://doi.org/10.1002/ett.4150
6. Tun H., Lupin S., Linn H.H., Lin K.N.Z. Selection the perimeter protection equipment in security systems // Proc. of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. P. 1504–1508. https://doi.org/10.1109/eiconrus.2018.8317383
7. Saxena A., Mueller C. Intelligent intrusion detection in computer networks using swarm intelligence // International Journal of Computer Applications. 2018. V. 179. N 16. P. 1–9. https://doi.org/10.5120/ijca2018916224
8. Liu G., Zhang J. CNID: Research of network intrusion detection based on convolutional neural network // Discrete Dynamics in Nature and Society. 2020. V. 2020. P. 1–11. https://doi.org/10.1155/2020/4705982
9. Wu Y., Wei D., Feng J. Network attacks detection methods based on deep learning techniques: A survey // Security and Communication Networks. 2020. V. 2020. P. 1–17. https://doi.org/10.1155/2020/8872923
10. Vincent P., Larochelle H., Bengio Y., Manzagol P.-A. Extracting and composing robust features with Denoising autoencoders // Proceedings of the 25th International Conference on Machine learning (ICML). P. 1096–1103. https://doi.org/10.1145/1390156.1390294
11. Vincent P., Larochelle H., Lajoie I., Bengio Y., Manzagol P.A. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion // Journal of Machine Learning Research. 2010. V. 11. P. 3371–3408.
12. Deng J., Zhang Z., Marchi E., Schuller B. Sparse autoencoder-based feature transfer learning for speech emotion recognition // Proc. of the 2013 Humaine Association Conference on Affective Computing and

Intelligent Interaction, 2013, pp. 511–516. https://doi.org/10.1109/acii.2013.90
13. Yan B., Han G. Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. *IEEE Access*, 2018, vol. 6, pp. 41238–41248. https://doi.org/10.1109/access.2018.2858277
14. Farahnakian F., Heikkonen J. A deep auto-encoder based approach for intrusion detection system. *Proc. of the 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 178–183. https://doi.org/10.23919/icact.2018.8323688
15. Shone N., Ngoc T.N. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018, vol. 2, no. 1, pp. 41–50. https://doi.org/10.1109/tetci.2017.2772792
16. Zhang C., Ruan F., Yin L., Chen X., Zhai L., Liu F. A deep learning approach for network intrusion detection based on NSL-KDD dataset. *Proc. of the IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 2019, pp. 41–45. https://doi.org/10.1109/icasid.2019.8925239
17. Al-Qatf M., Lasheng Y., Al-Habib M., Al-Sabahi K. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *IEEE Access*, 2018, vol. 6, pp. 2169–3536. https://doi.org/10.1109/access.2018.2869577
18. Zhang Y., Zhang Y., Zhang N., Xiao M. A network intrusion detection method based on deep learning with higher accuracy. *Procedia Computer Science*, 2020, vol. 174, pp. 50–54. https://doi.org/10.1016/j.procs.2020.06.055
19. Hinton G.E., Osindero S., Teh Y.-W. A fast learning algorithm for deep belief nets. *Neural Computation*, 2006, vol. 18, no. 7, pp. 1527–1554. https://doi.org/10.1162/neco.2006.18.7.1527
20. Ranzato M.A., Boureau Y.l., Cun Y.L. Sparse feature learning for deep belief networks. *Proc. of the 21st Annual Conference on Neural Information Processing Systems (NIPS)*, 2008, pp. 1185–1192.
21. Gao N., Gao L., Gao Q., Wang H. An intrusion detection model based on deep belief networks. *Proc. of the Second International Conference on Advanced Cloud and Big Data*, 2014, pp. 247–252. https://doi.org/10.1109/cbd.2014.41
22. Coli G.O., Aina S., Okegbile S.D., Lawal A.R., Oluwaranti A.I. DDoS attacks detection in the IoT using deep gaussian-bernoulli restricted boltzmann machine. *Modern Applied Science*, 2022, vol. 16, no. 2, pp. 12. https://doi.org/10.5539/mas.v16n2p12
23. Erpek T., Sagduyu Y.E., Shi Y. Deep learning for launching and mitigating wireless jamming attacks. *IEEE Transactions on Cognitive Communications and Networking*, 2019, vol. 5, no. 1, pp. 2–14. https://doi.org/10.1109/tccn.2018.2884910
24. Tang C., Luktarhan N., Zhao Y. SAAE-DNN: deep learning method on intrusion detection. *Symmetry*, 2020, vol. 12, no. 10, pp. 1695. https://doi.org/10.3390/sym12101695
25. Naseer S., Saleem Y., Khalid S., Bashir M.K., Han J., Iqbal M.M., Han K. Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, 2018, vol. 6, pp. 48231–48246. https://doi.org/10.1109/access.2018.2863036
26. Liu G., Zhang J. CNID: Research of network intrusion detection based on convolutional neural network. *Discrete Dynamics in Nature and Society*, 2020, vol. 2020, pp. 1–11. https://doi.org/10.1155/2020/4705982
27. Al-Emadi S., Al-Mohannadi A., Al-Senaid F. Using deep learning techniques for network intrusion detection. *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 171–176. https://doi.org/10.1109/iciot48696.2020.9089524
28. Graves A., Mohamed A.R., Hinton G. Speech recognition with deep recurrent neural networks. *Proc. of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 6645–6649. https://doi.org/10.1109/icassp.2013.6638947
29. Sutskever O., Vinyals Q.V., Le Q.V. Sequence to sequence learning with neural networks. *Proc. of the 27th International Conference on Neural Information Processing Systems (NIPS'14)*, 2014, pp. 3104–3112.
30. Thilagam T., Aruna R. Intrusion detection for network based cloud computing by custom RC-NN and optimization. *ICT Express*, 2021, vol. 2, no. 4, pp. 512–520. https://doi.org/10.1016/j.icte.2021.04.006
31. Prabhakaran V., Kulandasamy A. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. *Neural Computing and Applications*, 2021, vol. 33, no. 21, pp. 14459–14479. https://doi.org/10.1007/s00521-021-06085-5

Intelligent Interaction. 2013. P. 511–516. https://doi.org/10.1109/acii.2013.90
13. Yan B., Han G. Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system // IEEE Access. 2018. V. 6. P. 41238–41248. https://doi.org/10.1109/access.2018.2858277
14. Farahnakian F., Heikkonen J. A deep auto-encoder based approach for intrusion detection system // Proc. of the 20th International Conference on Advanced Communication Technology (ICACT). 2018. P. 178–183. https://doi.org/10.23919/icact.2018.8323688
15. Shone N., Ngoc T.N. A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2018. V. 2. N 1. P. 41–50. https://doi.org/10.1109/tetci.2017.2772792
16. Zhang C., Ruan F., Yin L., Chen X., Zhai L., Liu F. A deep learning approach for network intrusion detection based on NSL-KDD dataset // Proc. of the IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID). 2019. P. 41–45. https://doi.org/10.1109/icasid.2019.8925239
17. Al-Qatf M., Lasheng Y., Al-Habib M., Al-Sabahi K. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection // IEEE Access. 2018. V. 6. P. 2169–3536. https://doi.org/10.1109/access.2018.2869577
18. Zhang Y., Zhang Y., Zhang N., Xiao M. A network intrusion detection method based on deep learning with higher accuracy // Procedia Computer Science. 2020. V. 174. P. 50–54. https://doi.org/10.1016/j.procs.2020.06.055
19. Hinton G.E., Osindero S., Teh Y.-W. A fast learning algorithm for deep belief nets // Neural Computation. 2006. V. 18. N 7. P. 1527–1554. https://doi.org/10.1162/neco.2006.18.7.1527
20. Ranzato M.A., Boureau Y.l., Cun Y.L. Sparse feature learning for deep belief networks // Proc. of the 21st Annual Conference on Neural Information Processing Systems (NIPS). 2008. P. 1185–1192.
21. Gao N., Gao L., Gao Q., Wang H. An intrusion detection model based on deep belief networks // Proc. of the Second International Conference on Advanced Cloud and Big Data. 2014. P. 247–252. https://doi.org/10.1109/cbd.2014.41
22. Coli G.O., Aina S., Okegbile S.D., Lawal A.R., Oluwaranti A.I. DDoS attacks detection in the IoT using deep gaussian-bernoulli restricted boltzmann machine // Modern Applied Science. 2022. V. 16. N 2. P. 12. https://doi.org/10.5539/mas.v16n2p12
23. Erpek T., Sagduyu Y.E., Shi Y. Deep learning for launching and mitigating wireless jamming attacks // IEEE Transactions on Cognitive Communications and Networking. 2019. V. 5. N 1. P. 2–14. https://doi.org/10.1109/tccn.2018.2884910
24. Tang C., Luktarhan N., Zhao Y. SAAE-DNN: deep learning method on intrusion detection // Symmetry. 2020. V. 12. N 10. P. 1695. https://doi.org/10.3390/sym12101695
25. Naseer S., Saleem Y., Khalid S., Bashir M.K., Han J., Iqbal M.M., Han K. Enhanced network anomaly detection based on deep neural networks // IEEE Access. 2018. V. 6. P. 48231–48246. https://doi.org/10.1109/access.2018.2863036
26. Liu G., Zhang J. CNID: Research of network intrusion detection based on convolutional neural network // Discrete Dynamics in Nature and Society. 2020. V. 2020. P. 1–11. https://doi.org/10.1155/2020/4705982
27. Al-Emadi S., Al-Mohannadi A., Al-Senaid F. Using deep learning techniques for network intrusion detection // IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). 2020. P. 171–176. https://doi.org/10.1109/iciot48696.2020.9089524
28. Graves A., Mohamed A.R., Hinton G. Speech recognition with deep recurrent neural networks // Proc. of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. 2013. P. 6645–6649. https://doi.org/10.1109/icassp.2013v.6638947
29. Sutskever O., Vinyals Q.V., Le Q.V. Sequence to sequence learning with neural networks // Proc. of the 27th International Conference on Neural Information Processing Systems (NIPS'14). 2014. P. 3104–3112.
30. Thilagam T., Aruna R. Intrusion detection for network based cloud computing by custom RC-NN and optimization // ICT Express. 2021. V. 2. N 4. P. 512–520. https://doi.org/10.1016/j.icte.2021.04.006
31. Prabhakaran V., Kulandasamy A. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection // Neural Computing and Applications. 2021. V. 33. N 21. P. 14459–14479. https://doi.org/10.1007/s00521-021-06085-5

32. Al-Yaseen W.L. *Multiagent System for an Adaptive Real Time Intrusion Detection System*. LAP Lambert Academic Publishing, 2016, 272 p.

32. Al-Yaseen W.L. Multiagent System for an Adaptive Real Time Intrusion Detection System. LAP Lambert Academic Publishing, 2016. 272 p.

Authors

Duaa Wahab Al-Safaar — Magister, Lecturer, University of Babylon, Babylon, 51002, Iraq, https://orcid.org/0000-0002-2995-2342, duaa.raheem.gsci6@student.uobabylon.edu.iq
Wathiq Laftah Al-Yaseen — Associate Professor, D.Sc., Head of Computer Center, Technical Institute of Karbala, Karbala, 56001, Iraq; Head of Computer Center, Al-Furat Al-Awsat Technical University, Karbala, 56001, Iraq, SC 57188754655, https://orcid.org/0000-0002-2155-2993, wathiq@atu.edu.iq

Авторы

Аль-Сафар Дуа Вахаб Рахим — магистр, лектор, Вавилонский университет, Кербала, 51002, Ирак, https://orcid.org/0000-0002-2995-2342, duaa.raheem.gsci6@student.uobabylon.edu.iq
Аль-Ясин Ватик Лафтах — доцент, доктор наук, руководитель компьютерного центра, Технический институт Кербелы, Кербела, 56001, Ирак; руководитель компьютерного центра, Технический университет Аль-Фурат Аль-Авсат, Кербела, 56001, Ирак, SC 57188754655, https://orcid.org/0000-0002-2155-2993, wathiq@atu.edu.iq

Received 01.12.2022
Approved after reviewing 26.01.2023
Accepted 14.03.2023

Статья поступила в редакцию 01.12.2022
Одобрена после рецензирования 26.01.2023
Принята к печати 14.03.2023