IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 29, 2021, accepted June 27, 2021, date of publication July 14, 2021, date of current version July 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3097247

Deep Learning-Based Intrusion Detection Systems: A Systematic Review

JAN LANSKY[1], SAQIB ALI[2], MOKHTAR MOHAMMADI[3], MOHAMMED KAMAL MAJEED[4], SARKHEL H. TAHER KARIM[5], SHIMA RASHIDI[6], MEHDI HOSSEINZADEH[7], AND AMIR MASOUD RAHMANI[8]

[1]Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, 10100 Prague, Czech Republic
[2]Department of Information Systems, College of Economics and Political Science, Sultan Qaboos University, Muscat 123, Oman
[3]Department of Information Technology, College of Engineering and Computer Science, Lebanese French University, Erbil 44001, Iraq
[4]Department of Information Technology, Tishk International University, Erbil 44024, Iraq
[5]Computer Department, College of Science, University of Halabja, Halabja 46018, Iraq
[6]Department of Computer Science, University of Human Development, Sulaymaniyah 07786, Iraq
[7]Pattern Recognition and Machine Learning Lab, Gachon University, Seongnamdaero, Sujeonggu, Seongnam 13120, Republic of Korea
[8]Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan

Corresponding authors: Mehdi Hosseinzadeh (mehdi@gachon.ac.kr) and Amir Masoud Rahmani (rahmania@yuntech.edu.tw)

This work was supported by the University of Finance and Administration through the institutional support for long-term conceptual development of research of ''System approach to selected information and communications technology trends'' under Standard Project 7429/2020/02.

ABSTRACT Nowadays, the ever-increasing complication and severity of security attacks on computer networks have inspired security researchers to incorporate different machine learning methods to protect the organizations' data and reputation. Deep learning is one of the exciting techniques which recently are vastly employed by the IDS or intrusion detection systems to increase their performance in securing the computer networks and hosts. This survey article focuses on the deep learning-based intrusion detection schemes and puts forward an in-depth survey and classification of these schemes. It first presents the primary background concepts about IDS architecture and various deep learning techniques. It then classifies these schemes according to the type of deep learning methods utilized in each of them. It describes how deep learning networks are utilized in the intrusion detection process to recognize intrusions accurately. Finally, a complete analysis of the investigated IDS frameworks is provided, and concluding remarks and future directions are highlighted.

INDEX TERMS Intrusion detection, auto-encoder, recurrent neural network, Boltzmann machine, CNN.

I. INTRODUCTION

The widespread expansion of the computer networks and their new emerging applications have enabled the attackers to launch various security attacks against them by various means. In this context, Figure 1 depicts the percentage of the security attacks collected from McAfee Labs in 2017, in which most of them are browser attacks, brute force attacks, and Distributed Denial of Service (DDoS) attacks [1], [2]. Also, several security attacks for the new computing environments such as WBANs [3]–[5], e-healthcare systems [6]–[8], fog computing [9], Mobile Edge Computing (MEC), Cloud Computing [10], [11], wireless sensor networks [12], [13], mobile ad hoc networks [14]–[16], and SDNs [17]–[19] are conducted. Intrusion detection systems are crucial security components used in combination with firewalls to make the computer networks safer places for owning IT organizations and their customers [20], [21].

IDS solutions are one of the key security components that in combination with firewalls can effectively handle various types of security attacks. IDS schemes can be mainly classified as misuse detection schemes and anomaly detection schemes, which can be realized by using various machine learning techniques. Misuse detection or signature-based systems heavily depend on the signature of the security attacks and malicious behaviors and support multi-class classification. However, they cannot detect the new attacks in which their signature is not available for the IDS [22], [23]. However, as an advantage, these schemes benefit from more accuracy in recognizing known

The associate editor coordinating the review of this manuscript and approving it for publication was Yongqiang Cheng.

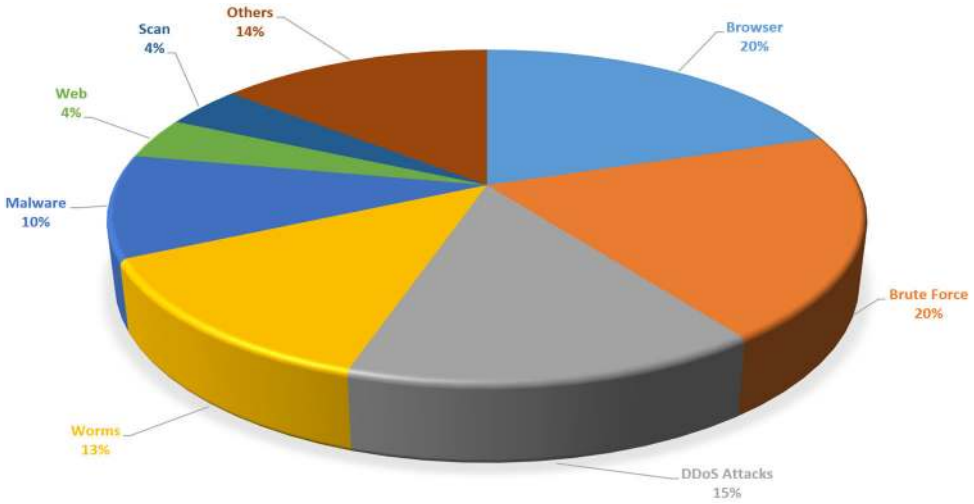


FIGURE 1. Security attacks in MacAfee network in 2017 [37].

malicious behaviors and their variants. On the other hand, the anomaly detection-based IDS approaches can detect new attacks by relying on the users' normal behavior profiles [24], [25] and only support binary classifications. Nonetheless, in dynamic organizations in which users' roles change occasionally, their profiles should be updated correspondingly [26]. Also, anomaly detection schemes may suffer from the false positive problem [27]–[30]. A large number of recent researches are conducted in both anomaly detection and misuse detection contexts using various machine learning techniques [31]–[35]. Conventional machine learning techniques suffer from the lack of labeled training datasets and heavily rely on the extracted features by a human, which makes it difficult for deployment on large platforms [36]. Deep learning is a novel paradigm in the machine learning field mainly established using ANNs or artificial neural networks and has a higher performance than the other conventional machine learning techniques.

Deep learning consists of various networks such as Convolutional Neural Networks (CNNs), Deep Belief Networks (DBNs), Restricted Boltzmann Machines (RBMs), and Recurrent Neural Networks (RNNs), each of which has different capabilities and properties. These networks can carry out the learning process in unsupervised, semi-supervised, or supervised manners [38]. Besides, they benefit from the hierarchical layers aimed to find proper high-level features from the raw input data instead of using manual features [36], [39]–[42]. Recently, deep learning techniques are successfully applied in various domains such as text, audio, and visual processing [43] as well as contexts such as sentiment analysis [44], social network analysis, recommender systems [45], natural language processing, wireless networking [46], and so on. Besides, deep learning has achieved a great deal of attention in the IDS context, and numerous deep learning-based misuse detection and anomaly detection models are provided in the literature to deal with various types of intrusions and security attacks. Although deep anomaly detection schemes and deep intrusion detection (both categories) schemes are studied by previously published review articles [47]–[54], no survey paper is specially presented in the literature to put forward a thorough investigation of the deep misuse detection-based intrusion detection approaches. Moreover, our work studies more intrusion detection schemes and presents a more in-depth comparison of the studied research.

For this purpose, this article focuses on deep learning-based intrusion detection and provides a thorough survey of the different frameworks published in this context from 2010 up to 2020. However, to be more useful before presenting the survey, it first introduces the key terms and background knowledge about the IDS schemes and briefly describes the leading deep learning techniques used in different steps of the intrusion detection process, such as feature selection/extraction and classification. To be more specific, this work classifies the deep intrusion detection approaches based on the type of deep learning network applied in their various intrusion detection steps. It also illuminates their significant contributions and security services, which each scheme provides. Furthermore, it describes their main steps carried out using deep learning methods. Besides, each section of the survey puts forward a comparison of the datasets, evaluation metrics, simulators, environments, and different feature extractions that have been applied in the analysis and verification of the proposed deep intrusion detection schemes. Such comparisons of the studied solutions can be beneficial in highlighting plans for future works and illuminating the areas which have been less investigated. According to our studies, this is the first paper aimed to explore intrusion detection schemes that use deep learning networks. The contribution of this survey article can be listed as follows:

- Discussing the key concepts in the intrusion detection process and illustrating the main categories of deep learning techniques.
- Categorizing the investigated deep IDS schemes regarding their utilized deep learning network.
- Demonstrating the key contributions, findings, and advantages of recent research conducted in the deep IDS context and comparing their evaluated metrics, simulators/environments, feature extraction methods, and datasets.
- Identifying critical challenges for the deep learning-based intrusion detection approaches, which should be handled in future researches.
- Providing useful information for researchers who investigate in deep IDS context and seek technical directions and knowledge for the development of their research work.

The remaining of this survey article is provided as follows: Section 2 articulates the key issues and background knowledge about the various IDS features and briefly describes the well-known deep learning models. Section 3 provides the classification of the studied schemes and reviews them. The comparison results are given in Section 4, and finally, concluding remarks and open research issues are outlined in Section 5.

II. RESEARCH METHODOLOGY

This section introduces the systematic literature review methodology [55] conducted for the deep learning-based misuse detection schemes proposed in the security literature. It describes the process of paper selection and highlights the research questions which will be addressed in the next sections. In this process, we selected the articles as follows:

- Regarding the deep learning and misuse detection context.
- Using the research context some search strings are selected and searched to find the required articles.

At first, for finding review articles in the intrusion detection context, we searched these strings:

- Intrusion Detection Survey
- Intrusion Detection Review
- Intrusion Detection Overview
- Anomaly Detection Survey
- Anomaly Detection Review
- Anomaly Detection Overview
- Misuse Detection Survey
- Misuse Detection Review
- Misuse Detection Overview

These searches resulted in some interesting review articles referenced in the introduction of this paper. For finding survey articles in the deep learning-based misuse detection context, we searched the following strings:

- Deep Learning Misuse Detection Survey
- Deep Learning Intrusion Detection Review
- Deep Learning Intrusion Signature Detection Review

TABLE 1. Applied libraries.

Index	Site	URL
1	Emerald	http://www.emeraldinsight.com
2	Springer	http://link.springer.com
3	Hindawi	https://www.hindawi.com
4	ACM	http://www.acm.org
5	Wiley	http://onlinelibrary.wiley.com
6	Inderscience	http://www.inderscience.com
7	IET Digital Library	https://digital-library.theiet.org
8	Science Direct	http://www.sciencedirect.com
9	IEEE explorer	http://ieeexplore.ieee.org
10	Sage	http://journals.sagepub.com

However, we found no paper satisfying these search strings. Likewise, for finding the new proposals and research articles in the deep learning-based misuse detection context, the following strings are searched:

- Auto Encoder Intrusion Detection
- Auto Encoder Misuse Detection
- Restricted Boltzmann Machines Intrusion Detection
- Restricted Boltzmann Machines Misuse Detection
- Recurrent Neural Networks Intrusion Detection
- Recurrent Neural Networks Misuse Detection
- Deep Neural Network Intrusion Detection
- Deep Neural Network Misuse Detection
- Convolutional Neural Networks Intrusion Detection
- Convolutional Neural Networks Misuse Detection
- Deep Belief Networks Intrusion Detection
- Deep Belief Networks Misuse Detection

The results achieved from these searches are screened to find credible and original articles. For example, documents such as thesis, patents, and papers from the journals which are not provided by the publishers listed in Table 1 are excluded. The remaining articles are used in conducting this review which will be reviewed in the next section. Figure 2 depicts the number of deep learning-based misuse detection schemes published from 2010 up to 2020. As shown in this figure, the number of these schemes is increasing and this context can be considered as an active research area. Furthermore, Table 2 describes the main research questions which have been addressed in this paper and the reasons which they are pursued. These questions can be useful for finding open issues in the deep learning-based misuse detection context and directing future researches in the proper directions. Figure 3 exhibits the percentage of the articles applied from different publications. As shown in this figure, most of the studied articles in this survey are achieved from the IEEE, Elsevier, and Springer publications.

III. PROPOSED DEEP LEARNING-BASED IDS SCHEMES

This section presents a review of the intrusion detection schemes [56]–[65], [67]–[69], which have benefited deep learning techniques in the security literature. It intends to answer some of the research questions specified in

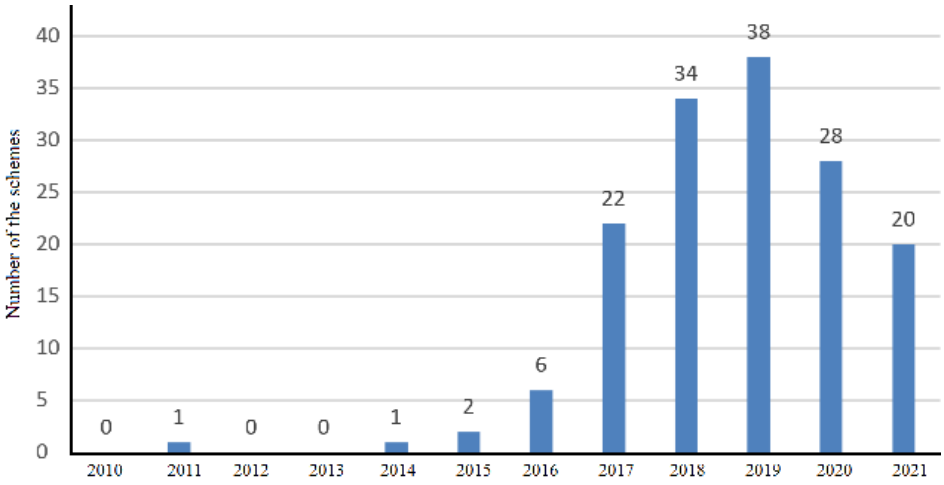


FIGURE 2. Number of deep learning-based misuse detection schemes.

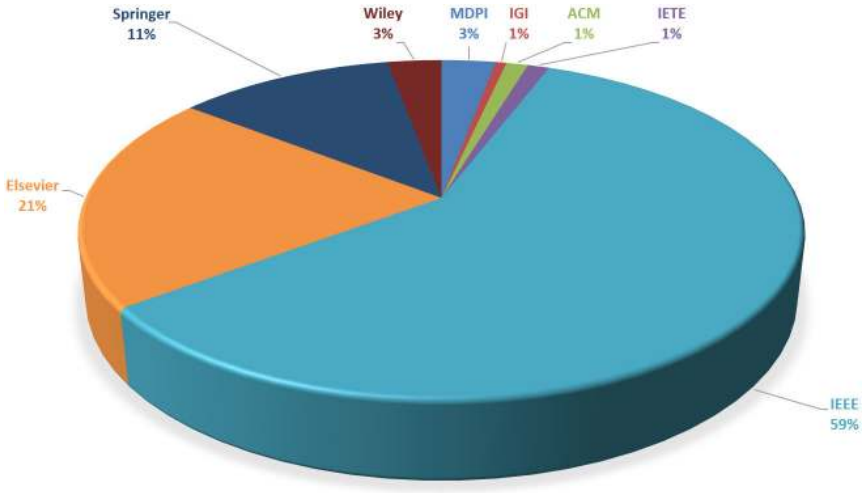


FIGURE 3. Percentage of the articles applied from different publications.

Section 2. Figure 4 indicates the classification of the deep learning-based IDS schemes according to the type of deep learning network utilized in them. Generally, the studied intrusion detection schemes employ deep learning techniques in the feature extraction step, the classification step, or both.

A. AUTO-ENCODER BASED SCHEMES

This subsection investigates the recently proposed auto-encoder-based intrusion detection schemes such as [69]–[83]. For instance, a deep learning-based scheme to handle intrusions is presented in [84] by Al-Qatf *et al.*, denoted as STL-IDS. This scheme uses the self-taught learning framework for the learning of features and reduction of dimension. This IDS model benefits from a sparse auto-encoder for unsupervised reconstructing a new feature representation. After the pre-training stage, the new features are used in the support vector machines (SVM) classifier to improve its detection accuracy. The efficiency of this approach in binary and multiclass classifications is evaluated against the naive Bayes, J48, SVM, and random forest classifiers, which are shallow. The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classifications and improves the prediction accuracy of the SVM. However, this can be further evaluated using GPU acceleration and parallel platforms. Also, in [85], the authors introduced an IDS approach that uses SVM and deep learning to improve intrusion detection performance. They utilized a stacked auto-encoder to decrease features and applied the SVM classifier for events classification into normal or attacks. They used ISCX 2012 dataset and achieved ten features from it by using an auto-encoder and fed it to the SVM for its training. The authors indicated the benefits of their method regarding metrics like Kappa statistic, detection rate, accuracy, and FPR. This scheme achieves a low FPR while keeping accuracy and precision higher. Although their method's performance is higher than the PCA-Gaussian mixture modeling method, it is only able to conduct the binary classification and cannot handle the multiclass attack traffics.

TABLE 2. The study questions.

Index	Question	Reason
1	Which major contributions are provided by each deep learning-based misuse detection framework?	Determines the open issues which each scheme is trying to solve. For instance, the deep learning techniques may be used by the IDS scheme for dimension reduction or classification purposes in a general or special environment.
2	Which kinds of deep learning models are used in each studied scheme?	This question illuminates the deep learning techniques applied in the feature extraction phase or in the classification phase applied to deal with the misuse detection problem. It is answered in the description of each scheme provided in section 4.
3	Which kinds of shallow learning methods are used in combination with the deep learning models to deal with the misuse detection problem? Or in the evaluation process?	This question illuminates the shallow learning methods which have been applied in the studied misuse detection schemes and results that have been achieved by such integrations. The answer to this question is provided in section 4, where each scheme is described.
4	Which datasets are supported by each studied deep learning-based misuse detection scheme?	Not all investigated schemes apply raw traffic data for intrusion detection. This question outlines the applied datasets in the misuse detection process in the studied schemes. By having this knowledge, the new researchers can recognize the popular datasets and the issues which should be dealt with them by using these datasets. The answer to this question is provided in the comparison tables of section 4.
5	Which simulators are employed by the studied deep learning-based misuse detection approaches?	This question determines the tools applied to simulate the deep learning-based IDS schemes. The results achieved by this question can be very useful in selecting special-purpose software environments that can improve the development speed of the new proposals. This question is answered in the comparison tables provided in section 4.
6	Which factors are considered in the evaluation and analysis of the investigated misuse detection?	Different metrics are used by the studied misuse detection solutions in the simulation process, which identifying them is useful for designing new IDS solutions and exploring other important factors. This question is also answered in the comparison tables provided in Section 4.

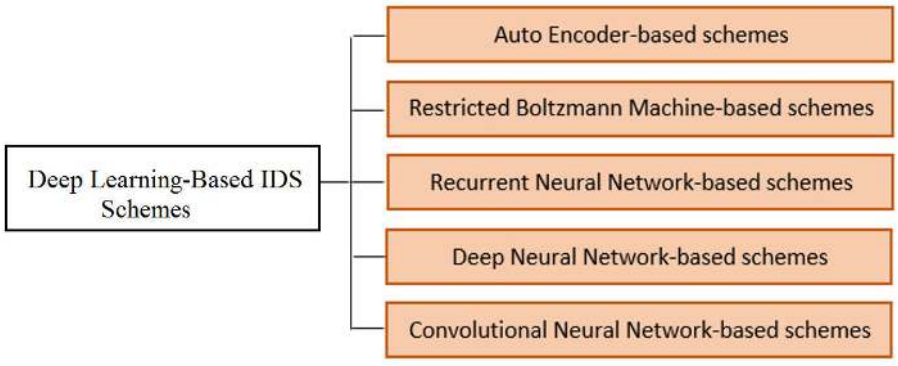


FIGURE 4. Classification of the deep learning-based intrusion detection schemes.

Auto-encoder is one of the methods applied to find appropriate features in the investigated schemes. As an example, in [86], Farahnakian *et al.* put forward DAE-IDS, which is a deep learning-based IDS method that employs a deep auto-encoder, trained by a greedy layer-wise method to prevent problems such as local optimum and over-fitting. It consists

of four layers of auto-encoders in which the output of each layer is fed to the input of another layer. Also, a greedy unsupervised layer-wise training method is utilized for training DAE-IDS, enhancing the performance of a deep model. An auto-encoder at the current layer is trained before the auto-encoder at the next layer. After training four auto-encoders, they used a softmax classifier to categorize the inputs into the normal and attack classes. The authors conducted their experiments on the KDDCup99 dataset and demonstrated that it could improve accuracy, detection rate, and FPR. However, the sparsity constraints are not explored on the auto-encoders, and how sparse deep auto-encoders can be used to improve the IDS performance is not discussed.

Yu *et al.* [87] provided a session-based network IDS using a deep learning-based scheme and achieved excellent performance in recognizing botnet traffics. They implemented a deep architecture to learn features of the botnet traffics and introduced a method to create a dataset from raw network traffics. The authors indicated that deep learning approaches are useful in the session-based network IDS. However, the deep architecture's parameters, such as the number of hidden layers, should be tuned further.

In [88], Niyaz *et al.* presented a multi-vector DDoS attack detection system based on deep learning for the SDN and implemented it on the SDN controllers as an application. It applies deep learning for the reduction of features achieved directly from the traces of various network traffic. A sparse auto-encoder is a neural network that consists of three layers. They evaluated their system based on traffic traces collected from different scenarios. But, they did not address issues such as bottleneck problems at the controller and also did not considered different types of DDoS attacks. However, this scheme cannot work with raw traffic and depends on the derived features. Besides, the proposed approach in [89] provided a distributed deep learning-based attack detection scheme for the fog computing environment by applying the NSL-KDD. In this scheme, a pre-trained stacked auto-encoder is employed to reduce features, and the softmax classifier is applied for classification purposes. They compared their model with shallow learning methods and analyzed its results using metrics such as DR, accuracy, training time, testing time, and ROC curve. As outlined by the authors, this scheme must be further evaluated on other datasets and should be compared with other types of neural networks.

Shone *et al.* [90] presented an IDS scheme, in which unsupervised feature learning applies a non-symmetric deep auto-encoder. They provided a classification method by incorporating the stacked non-symmetric deep auto-encoders and the random forest classifier. They analyzed their model with the Tensor Flow software tool and applied the NSL-KDD and KDDCup99 datasets. The authors compared their approach against the DBN and indicated that their approach provides higher accuracy, precision, and recall while reducing training time.

The intrusion detection approach in [91] provided a de-noising approach combined with the deep learning methods to deal with the imbalanced datasets applied in the network IDSs. The authors applied the NSL-KDD dataset and carried out their experiments using TensorFlow and used their denoising method to improve results achieved by the SAE and DBN. The authors showed that their method could improve recall, precision, and accuracy while balancing accuracy for the U2R and R2L attacks. However, further evaluations of real traffics are needed to verify the capabilities of this IDS approach.

In [92], the authors established a network IDS using deep learning, which applies power-efficient Neuromorphic processors. They encoded the data to train the auto-encoder, and its achieved weights are involved in the supervised training step. At last, the weights are converted to discrete values by applying discrete vector factorization to produce synaptic weights and crossbar weights, as well as neurons' thresholds. This IDS model is analyzed with the Neurosynaptic core simulator, and the results indicated that it benefits from high accuracy with low power usage.

In [93], Kim *et al.* introduced DAEQ-N, which utilizes a reinforcement learning-based method that uses a deep auto-encoder in the Q-network to achieve high prediction accuracy in online learning systems while detecting intrusions by verifying whether the data is classified as normal or anomalous. In their model, the rewards are calculated as the sums of the differences between encoding and decoding. They developed the average reward during the training and achieved steady progress using the auto-encoder. The relevant feature patterns are fed back into the DAEQ-N.

Furthermore, the network IDS proposed in [94] utilized the self-taught learning method for training the deep neural network. They indicated that the concatenation of the features extracted by self-taught learning with the NSL-KDD's features increases the performance of the sparse auto-encoder. The IDS scheme's performance is compared regarding the accuracy, detection rate, FPR, precision-recall curve, and ROC.

Also, in [95], Louati and Ktata introduced DL-MAFID, for solving multi-class intrusion detection problems using multi-agent systems and auto-encoder. This scheme uses an auto-encoder for dimension reduction and evaluates its dimension reduction capability using the KDDCup'99 dataset. Besides, shallow classifiers such as MLP and KNN are used to recognize five classes of the studied dataset. The conducted experiments showed that DL-MAFID can achieve an accuracy of 99.95% and decreases the detection time.

Abusitta *et al.* [70], proposed a deep learning-driven IDS scheme for multi-cloud environments that can handle incomplete IDS feedbacks. More specifically, it learns to reconstruct IDS feedbacks regarding incomplete feedbacks using the denoising auto-encoder. Besides, this scheme learns extracting features that can handle incomplete feedback, allowing deciding about probable intrusions regarding the incomplete IDS feedback. The authors evaluated their scheme using the KDDCup'99 dataset in the GPU-enabled TensorFlow against MLP and stacked auto-encoder.

TABLE 3. Evaluation parameters applied in Auto-Encoder based IDS schemes.

	Evaluation metrics											Simulators/Tools/ Programming Languages					Datasets				
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	F-measure	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	KDDCup99	NSL-KDD	DARPA	ISCX	Self-Collected
[70]					✓									✓			✓				
[71]		✓			✓	✓	✓	✓				✓									
[72]					✓	✓	✓	✓		✓	✓			✓			✓	✓			
[73]					✓	✓	✓	✓						✓				✓			
[84]	✓	✓	✓	✓	✓	✓	✓	✓										✓			
[85]					✓	✓					✓				✓					✓	
[86]					✓					✓	✓		✓				✓				
[74]	✓			✓					✓					✓							✓
[87]				✓	✓	✓	✓	✓				✓								✓	
[88]				✓	✓	✓	✓	✓													✓
[89]		✓		✓	✓					✓	✓			✓				✓			
[90]	✓	✓	✓	✓	✓	✓	✓	✓			✓				✓	✓	✓	✓			
[75]					✓	✓	✓	✓						✓				✓			
[91]	✓	✓	✓	✓	✓	✓	✓	✓					✓					✓			
[92]					✓									✓			✓				
[93]														✓							✓
[76]	✓	✓	✓	✓	✓																✓
[94]	✓	✓	✓	✓	✓	✓	✓			✓	✓							✓			
[95]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓		✓				
[96]														✓				✓			

Uneven distribution of data can happen in training, to deal with this issue, in [96], Chuang and Wu presented a NIDS scheme in which applies a data generation model by training a variational auto-encoder to deal with data shortage and imbalanced data in datasets. For training the NID model, this scheme applies a data generation model to provide a dataset with a balanced set of records for each category of attacks. By having a balanced dataset, the over-fitting problem in the training of the proposed IDS model can be handled. The authors have evaluated their scheme using the Keras and apply the NSL-KDD dataset. Table 3 compares the evaluation metrics, simulators, feature extractions, and datasets applied in the auto-encoder-based intrusion detection schemes investigated in this part of the paper.

B. RESTRICTED BOLTZMANN MACHINE-BASED SCHEMES

Many schemes have used RBM in the detection of intrusions [97]–[99]. For example, in [100], the authors provided an IDS framework for smart cities by using RBMs for unsupervised learning of the features from data generated by sensors. By using achieved features, various classifiers are trained. They used the RBM models with various layers and indicated the ability of the automated feed-forward ANN in outperforming the feed-forward ANNs, random forest, and SVM learned models. The authors indicated the efficiency of their method in detecting attacks with higher accuracy. However, they also demonstrated that the performance of attack detection decreases as the number of classes ascends. Also, the security scheme in [98] provided RBC-IDS, an RBM-based, and clustering-based IDS for WSNs. They studied its performance and compared it to another IDS scheme called ASCH-IDS. The authors indicated that ASCH-IDS and RBC-IDS could reach the same accuracy and detection rate, but the RBCIDS's detection time is longer. They also used the various number of hidden layers in the RBC-IDS compared it against the ASCH-IDS. They exhibited that when their scheme is used with three hidden layers, it can achieve a higher detection rate and accuracy. Besides, they showed that the machine learning IDS solutions perform the same as the deep learning IDS schemes, but with less detection time.

Also, Zhang *et al.* [101] introduced an IDS framework by combining RBM, SVM, and DBN and the combination of the ANNs at the bottom, aiming to improve the accuracy and speed of the RBM. Unsupervised learning can enhance the ANNs to extract features more efficiently. To evaluate their scheme, the authors applied metrics such as accuracy, FPR, FNR, testing time, and training time with the KDDCup99 dataset and indicated some improvements in these metrics. Besides, the network IDS introduced in [102] applied RBMs to learn various complex datasets. They analyzed the learning procedures of RBMs and trained their RBMs on the IDS datasets. Besides, Alom *et al.* [103] presented a network IDS

TABLE 4. Properties of the RBM-based intrusion detection schemes.

	Evaluation metrics											Simulators/Tools/ Programming Languages					Datasets				
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	F-measure	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	KDDCup99	NSL-KDD	DARPA	ISCX	Self-Collected
[100]								✓				✓									✓
[98]	✓				✓			✓		✓					✓		✓				
[97]					✓	✓	✓	✓						✓							
[101]	✓	✓			✓												✓				
[102]														✓						✓	
[103]														✓			✓				
[104]	✓	✓	✓	✓	✓						✓						✓				
[105]	✓	✓	✓	✓	✓	✓	✓	✓		✓							✓				

using unsupervised deep learning and rules-based approaches to identify new types of attacks. In this scheme, the auto-encoder and RBM are applied for the unsupervised extraction of features. Then k-means clustering is applied to these three features, and an unsupervised extreme learning machine is used in network IDS. The authors carried out the KDD-Cup99 dataset and achieved high detection accuracy. Another network IDS approach is proposed in [104], which benefits from deep confidence neural networks to find features of monitored network data and used BP neural network classifier to detect intrusions. The authors analyzed the influence of the DBN network model's parameters on the IDS performance. They also validated their scheme using the KDDCup99 dataset and indicated that it improves accuracy over the shallow learning methods. For recognizing DDoS attacks, in [105], Mayuranathan *et al.* proposed RHS-RBM, an IDS model based on the feature selected using a random harmony search optimization model. After the feature selection step, this scheme applies a classifier model using RBM for detecting DDoS attacks. For increasing DDoS attacks' detection rate, seven layers are added to the RBM model and its parameters are optimized to achieve better results. The authors performed their experiments using the KDDCup'99 dataset and achieved 99.88 for sensitivity, 99.96 for specificity, 99.93 for F1-Score, 99.92 for accuracy, and 99.84 for kappa. These achieved results indicated that RHS-RBM is better than the RBM model. Table 4 compares the evaluation metrics, simulators, feature extractions, and datasets applied in the RBM-based intrusion detection schemes investigated in this part of the paper.

C. DEEP BELIEF NETWORK-BASED SCHEMES

This subsection discusses the IDS schemes [106]–[113], which have utilized the DBN in handling intrusions and security vulnerabilities. For instance, Zhang *et al.* [114] presented an IDS approach based on the DBN and an improved GA, which intends to find an optimal network structure for DBN to classify security attacks. It reduces the network structure complexity and enhances the accuracy of classification.

Also, for attacks such as U2R, which have fewer training data, their approach provides higher accuracy than other methods. They optimized the deep network parameters, reduced the training time, and improved the IDS accuracy.

In [115], Gao *et al.* introduced an IDS model based on the DBN, which combines a back-propagation network and RBM. The deep learning model proposed in this scheme can learn high-dimensional representations and performs the classification task. Besides, this scheme uses the unsupervised greedy learning algorithm for pre-training and also tuning the DBN to learn high-dimensional data and facilitate the classification.

The intrusion detection approach proposed in [116] investigated the abilities of the DBN in conducting intrusion detection on the NSL-KDD after its training. The authors evaluated the training time and testing time of their system and indicated that it could recognize the security attacks and classifies them into five classes in the presence of incomplete and nonlinear data.

Tian *et al.* [117] tried to improve the IDS accuracy by using recursive DBNs and random forest classifiers. They introduced the forgetting coefficient and the tracking time-varying factor to make the trained parameters reasonable. They also classified the extracted features using the random forest classifier and indicated that it could increase the detection rate and reduce the FPR. Besides, David *et al.* [118] provided a hybrid IDS scheme by using deep learning techniques for the generation of the security attacks' signatures and classifying them. This scheme employs a deep stack of denoising AEs for implementing DBN, which can process raw input data for training the DNN and generate malware signatures. Their approach achieves a high level of accuracy by using the DBN-generated signatures and uses a dataset containing primary malware attacks.

TABLE 5. Comparison of the DBN-based intrusion detection approaches.

	Evaluation metrics										Simulators/Tools/Programming Languages						Datasets			
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	PCA	NSL-KDD	DARPA	ISCX	Self-Collected
[114]					✓	✓	✓		✓	✓					✓		✓			
[115]		✓		✓	✓			✓	✓	✓				✓						
[116]					✓									✓			✓			
[117]		✓							✓				✓							
[118]												✓								
[119]													✓			✓	✓			
[120]		✓			✓	✓	✓		✓				✓			✓	✓			
[121]		✓	✓	✓		✓	✓							✓						✓

In [119], Salama *et al.* provided an IDS scheme that benefits from the DBN and SVM and can conduct network traffic classification into normal traffic class, U2R, DoS, R2L, and Probing attacks. They used DBN to mitigate the dimension of feature sets and used SVM to classify the intrusion. They presented tests on the NSL-KDD dataset and indicated that their approach accuracy is high.

The intrusion detection scheme proposed in [120] provided MDPCA-DBN, a fuzzy aggregation method that uses DBN, and a density peak clustering method. This scheme divides the training set to reduce dataset size and mitigate the imbalance of the data samples in the primary dataset. Each of the subsets is applied for training sub-DBNs and reducing data dimensions. They calculated the weights of the fuzzy membership function of the test samples in the sub-DBNs and aggregated their output according to their weights. The authors conducted experiments on the NSL-KDD and UNSW-NB15 IDS datasets to indicate that their scheme can improve metrics like recall, accuracy, precision, detection rate, F1-score, and FPR. The security solution in [121] developed an IDS for the IoT environment, which employs a deep learning method to recognize malicious traffics by providing security as a service and enabling interoperability in the IoT. They evaluated their scheme using raw traffic data achieved from the network traffic traces. Table 5 compares the evaluation metrics, simulators, feature extractions, and datasets applied in the DBN-based intrusion detection schemes, outlined in this subsection.

D. RECURRENT NEURAL NETWORK-BASED SCHEMES

This subsection studies the IDS schemes [110], [122]–[129], which apply RNN in the detection of intrusions. For instance, for detecting attacks within the IoT network, Roy *et al.* [130] incorporated an LSTM RNN. This scheme deals with the IoT traffic to recognize the attack and normal patterns. The authors trained the RNN with the UNSWNB15 dataset and indicated that their model's efficiency regarding metrics like recall, precision, FAR, and F-1 score. They noted that BLSTM RNN-based IDS is efficient and can have high accuracy. However, further experiments on the more massive datasets of IoT traffics should be conducted to verify the achieved results.

Yin *et al.* [131] introduced RNN-IDS, a deep learning-based method for detecting intrusions using RNNs.

They studied their scheme in the multiclass and binary classification problems and analyzed the neurons and various learning rates' impact on their model. This scheme is evaluated on the NSL-KDD against shallow classifiers like naive Bayesian, J48, and random forest, and it is indicated that it could achieve a high detection rate and accuracy with a low FPR in multiclass classification.

The IDS scheme in [132] applied real-time data as input to a neural network. They used a deep multilayer perceptron and also an RNN model, which benefits from an LSTM hidden layer for learning the temporal context of several attacks such as command injection and DDoS. Based on the detection latency, they introduced a mathematical model to determine the proper time for computation offloading of their model.

The DDoS attack detection approach presented in [133] uses deep learning to find the most useful features from the low-level features and achieves reasonable inference. In this scheme, the DDoS attack detection is formulated as a sequence classification, and the packet-based DDoS attack detection is transformed into window-based attack detection. In this scheme, the deep defense consists of RNN, CNN, and fully connected layers. They designed an RNN to learn traffic patterns, which improve the performance of DDoS detection and decrease the error rate. RNN can also learn long historical features and outperforms the random forest classifier. Nonetheless, to further verify the results of this RRN-based scheme, it should be tested on the datasets with several DoS attacks and compared with other shallow models.

In [134], Jiang *et al.* applied an LSTM RNN to conduct a multi-channel attack detection. To enhance the detection rate, it preprocesses data and performs feature abstraction and training, and detection steps. Preprocessing of data provides high-quality data, and then various features can be achieved from it. They trained the neural networks with multiple features and classified the attacks. They also introduced a voting algorithm that outperforms shallow classifiers such as Bayesian and SVM while classifying input data as normal or attack.

In [135], Kasongo *et al.* presented DLSTM, an IDS scheme that utilizes a deep LSTM-based classifier and benefits from the multiple LSTM layers coupled to a DFFL to find intrusions. Furthermore, this scheme applies the information gain method for selecting appropriate features. They used the NSL-KDD dataset and compared their approach against Naïve Bayes, SVM, random forests, KNN, and deep feed-forward neural networks. The authors improved the accuracy and F1-Score; nonetheless, as specified by them, more evaluations on other datasets and attacks are needed to verify the achieved results and improvements.

In [136], Kaur *et al.* provided D-Sign, a deep learning-based hybrid IDS scheme for intrusion detection, which can generate the signature of new web attacks. The evaluations of D-Sign are conducted using the ROC area, detection rate, precision, TPR, recall, F-measure, and FPR. The authors indicated that their scheme could improve sensitivity, accuracy, and specificity while reducing the FPR and FNR. However, to increase the performance of this scheme, a better pattern matching algorithm should be used for a signature generation while testing it with an updated dataset. Also, to prevent the vanishing gradient problem, the proposed RNN must be further improved.

In [137], Xu *et al.* proposed an IDS that consists of a softmax module, multilayer perceptron (MLP), and an RNN with gated recurrent units (GRU). This IDS approach is tested using the NSL-KDD and KDDCup'99 datasets. The experimental results showed that GRU provides better results than the LSTM in the RNNs and the bidirectional GRU achieves the best results. However, their system relies on theoretical verification, and to further verify it, this method must be applied to real network environments.

Almiani *et al.* [138], introduced an automated IDS for securing fog computing, which applies multi-layered RNN. This IDS model incorporates an improved backpropagation algorithm to train the RNN. This scheme has two engines denoted as classification and traffic analysis engines.

At first, the traffic connection records are pre-processed in the traffic processing unit to provide usable traffic data for the classification engine where the connections are classified into normal and attack. Furthermore, this IDS is analyzed using the NSL-KDD dataset and metrics such as accuracy, precision, detection rate, F1-measure, false-positive rate, false-negative rate, Kappa coefficients, and Mathew correlation. But, to verify the achieved results, further evaluations using real network traffic are necessary. Table 6 indicates the applied evaluation metrics, tools, feature extractions, and IDS datasets in the RNN-based intrusion detection schemes.

E. DEEP NEURAL NETWORK-BASED SCHEMES

This subsection studies the IDS schemes such as [139]–[149], which utilize the DNN in handling intrusions and security attacks. For instance, in [150], Amarasinghe *et al.* presented a supervised learning IDS scheme using DNN, which for increasing the trust of the users generates feedbacks on the decision-making of the IDS. This scheme generates offline feedback after the training process and creates online feedback in the deployment process. This scheme is evaluated using the NSL-KDD for detecting two DDoS and Probe attacks using different depths. The authors exhibited that their created feedback can add another evaluation layer by the user. However, the authors have not considered the speed of events into account in creating online feedback, and the feedback should be generated in human-understandable methods.

The intrusion detection scheme in [151] addressed the ability of DNN as a classifier for handling a diverse set of intrusions. The training and validation models have a high R2 value that indicates the introduced model can be accurate. With the loss being set as cross-entropy, they got a classification model to detect the next intrusions.

In [152], Kim *et al.* provided an IDS using a DNN, in which preprocess data using transformation and normalization. After refining the data by preprocessing, the DNN is used to create a learning model, and for conducting the required evaluations, the KDDCup99 is employed to analyze the accuracy, detection rate, and FPR of this model.

The work in [153] proposed an IDS scheme using a DNN and trained it by using packet traces exchanged among electronic control units in the vehicular network. They tried to find proper features generated from network data for detecting normal and attack packets. For providing a fast response to the security attacks with a high detection ratio, this IDS scheme monitors packet exchange in vehicular networks and trains the features offline. Also, they evaluated the required time for training and testing steps.

Potluri *et al.* [154] presented a DNN-based IDS scheme, which at first converts the non-numeric values to the numeric ones and then normalizes them. Afterward, the training is conducted on various multi-core systems, and the required time for training is analyzed. This IDS scheme utilizes the DNN to extract the relations between the given input data. Also, the tuning of the DNN is conducted after various training stages. Then, DNN classifies the input data into the normal and attack classes, and it also should be tested with the test part of the dataset. But, because there are a few training data for attacks such as U2R and R2L, these attacks are not detected, and this problem decreases the detection accuracy of this scheme. Also, they exhibited that the training step can be conducted faster by using the multicore CPU, but the GPU did not achieve high performance because of the applied data type. The security solution in [155] proposed an ensemble-based IDS which applies deep techniques

TABLE 6. Properties of the RNN-based intrusion detection schemes.

	Evaluation metrics											Simulators/Tools/Programming Languages					Datasets				
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	F-measure	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	KDDCup99	NSL-KDD	DARPA	ISCX	Self-Collected
[130]	✓	✓	✓	✓	✓	✓	✓	✓						✓							
[122]	✓	✓	✓	✓	✓	✓	✓	✓										✓			
[131]		✓		✓	✓							✓						✓			
[132]															✓						✓
[123]							✓														
[133]					✓	✓	✓	✓	✓						✓					✓	
[134]					✓					✓	✓			✓				✓			
[135]	✓	✓	✓	✓	✓	✓	✓							✓				✓			
[124]															✓						✓
[136]	✓	✓	✓	✓		✓	✓											✓			
[137]	✓	✓	✓	✓	✓	✓	✓	✓						✓			✓	✓			
[138]	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓						✓			

like auto-encoder, DNN, DBNN, and an extreme learning machine. It uses the NSL-KDD to study the performance of the implemented neural network ensemble based on metrics such as accuracy, detection rate, FPR, and AUC. To further improve the results, other machine learning approaches should be analyzed in the proposed ensemble. The IDS scheme in [156] tried to apply two kinds of DNNs, which are auto-encoder and RNN, to recognize payload-based web attacks. Their model utilizes two DNNs to find useful features and classify the URLs as benign or malicious.

In [157], the authors used recurrent and convolutional network layers to construct an ANN model for finding appropriate features. They provided a hierarchical extraction of features by integrating the convolution of n-grams with sequential modeling. By using one recurrent layer and two convolutional layers, they detect various malware.

The IDS approach in [158] utilized DNN for the classification of the security attacks on the internet of things and evaluated the performance of their scheme using datasets such as CIDDS-001, GPRS, and UNSW-NB15. Furthermore, the DNN is integrated with a grid search method to tune parameters for each dataset. They analyzed their approach's performance regarding metrics such as accuracy, recall, precision, and FPR.

Peng *et al.* [159] proposed ENIDS, a deep learning-based network IDS framework for improving IDS performance. It uses the NSL-KDD to train classifiers such as DNN, SVM, logistic regression models, and random forest. Nonetheless, the authors showed that their approach is vulnerable to some security attacks.

The IDS scheme in [160] is aimed to classify network traffic datasets by using classifiers such as random forest, gradient boosting tree, and deep feed-forward ANN. They used a homogeneity metric for finding the most appropriate features from a dataset. Besides, they utilized 5-fold cross-validation to assess their models. The authors demonstrated that their approach provides high accuracy for multiclass and binary classification with DNN on the CICIDS2017 and UNSW NB15 datasets.

The work in [161] provided TSDL, an IDS scheme based on a deep-stacked auto-encoder neural network that applies two hidden layers and the softmax classifier. This deep model is trained by a semi-supervised method, and each of the hidden layers is pre-trained unsupervised using the unlabeled traffic features. The initial decision step of this model classifies the network traffic into normal and abnormal classes using the deep learning model by the user. To recognize the attack types, where the probability of the initial step's output is utilized as a feature to complement the main features, and this further enables the decision-making step to classify various types of attacks. They evaluated their scheme on the datasets such as KDDCup99 and UNSWNB15, which have more types of attacks.

This model achieves good accuracy for multiclass intrusion detection with both datasets. Also, FAR and the execution time of this scheme are low. Table 7 indicates the evaluation metrics, tools, feature extractions, and datasets applied in the DNN-based schemes.

F. CNN-BASED SCHEMES

This subsection discusses the intrusion detection schemes such as [162]–[189], which apply CNN in intrusion detection. For example, in [190], Xiao *et al.* introduced CNN–IDS, a network IDS based on a CNN model. It extracts the

TABLE 7. Properties of the DNN-based intrusion detection schemes.

	Evaluation metrics											Simulators/Tools/Programming Languages					Datasets				
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	F-measure	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	KDDCup99	NSL-KDD	DARPA	ISCX	Self-Collected
[139]	✓	✓	✓	✓	✓	✓	✓	✓			✓			✓				✓			
[137]	✓	✓	✓	✓	✓	✓		✓		✓						✓	✓	✓			
[140]		✓		✓	✓	✓		✓							✓		✓	✓			✓
[141]																	✓				
[142]															✓			✓			
[143]					✓	✓	✓	✓							✓		✓				
[144]	✓	✓	✓	✓	✓	✓	✓				✓			✓			✓				
[150]												✓						✓			
[151]					✓				✓								✓				
[152]					✓					✓	✓			✓			✓				
[153]	✓	✓										✓									
[154]															✓			✓			
[148]					✓					✓	✓								✓	✓	
[146]					✓	✓	✓	✓							✓			✓			
[155]	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓						✓			
[156]					✓									✓							✓
[145]				✓	✓	✓	✓	✓				✓						✓			
[147]															✓						
[157]												✓									✓
[158]					✓	✓	✓				✓			✓							
[159]	✓	✓	✓	✓	✓	✓	✓							✓				✓			
[160]	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓								✓
[161]					✓			✓			✓				✓		✓				

network traffic features by using CNN, and then, the required data for detecting intrusions is achieved by supervised learning.

For decreasing the execution cost, in this scheme, the traffic vector is converted into an image. The authors used KDD-Cup99 for performance evaluation and showed that based on various metrics such as FAR, accuracy, and timeliness, the CNN–IDS model is good. However, the low detection rate of attacks such as R2L and U2R is not addressed in this scheme.

The security solution in [191] proposed a character-based IDS scheme using CNNs. It considers the network traffic as a set of characters and encodes them into a vector, aggregated into a matrix as the input of the CNNs. It uses the NSL-KDD for conducting the required experiments and shows that it has good accuracy, detection rate, and low FPR in binary and multiclass classification. However, the authors failed to investigate the impact of various structures of CNN on their model. Also, Wang *et al.* [192] provided an encrypted traffic classification approach using one-dimensional CNNs, which integrates the extraction and selection of features with a classifier. The authors have verified their scheme using ISCX VPN-nonVPN dataset. They demonstrated that the 1D-CNN can classifies encrypted traffic better than the 2D-CNN.

In [193], Saxe *et al.* presented the eXpose neural network, which employs a deep learning approach to receive short strings, learn useful features, and classify the input using character-level embedding and CNN. They developed a CNN for the automatic finding of features from a string. Using embedding with convolutions as top layers with the supervised training allows finding useful features optimized for classification. This scheme demonstrates how a deep-learning method is adapted to security problems, where strings are obfuscated to prevent the extraction of the features. However, in this scheme, the computational cost of training on the long strings is high.

The IDS approach in [194] presented a network traffic classification scheme using a CNN model, which considers the data traffic as images. In this approach, the classifier can handle raw network traffic data and does not need any features designed by a human. The scheme is evaluated using two different scenarios with three classifiers. In these experiments, the authors showed that their approach could obtain the required accuracy.

In [195], the authors introduced a few-shot deep learning scheme for improving IDS performance. They trained a deep CNN for IDS. They tried to extract various layers in the CNN model and applied a 1-nearest neighbor and linear SVM classifiers. It can deal with the imbalanced training samples problem in which a specific class has limited data. They used NSL-KDD and KDDCup99 datasets. But, this scheme should be further evaluated on the other imbalanced datasets, in which some of their attack classes have much fewer data records than others, to verify the detection rate of the minority class security attacks.

Yang *et al.* [196] are aimed to secure the SCADA networks against malicious attacks by proposing a deep-learning-based IDS. This approach employs a CNN-based model to find traffic patterns and time windows of network attacks. They designed a re-training scheme to deal with unseen attack instances, to update SCADA systems their neural networks with attack traces. Their experiments showed that this approach achieves good accuracy in handling network intrusions in the SCADA systems. However, this scheme does not support mixed attacks and should be enhanced to deal with other security attacks on the SCADA protocols.

In [197], Zeng *et al.* presented an IDS approach by using a deep learning-based model to recognize malware traffic for OBUs. This scheme does not need the extracted features by a human and, as an advantage, can handle raw traffic data. The performance of this scheme is compared against other IDS methods on a public dataset and on a simulated VANET dataset. The results indicated that this scheme could achieve excellent performance with a lower resource requirement.

Bassey *et al.* [198] applied deep learning in an IDS model to find unauthorized devices in IoT, by using radiofrequency fingerprinting(RF), which are hard to impersonate and are collected from six identical ZigBee devices. A CNN is used to find appropriate features from the RF traces, and de-correlation is performed on these features. The reduced features are clustered to identify IoT devices. The experimental results exhibited that the deep learning-based extraction of feature can recognize new machines which were not observed in the training step.

The security approach proposed in [199] introduced an IDS based on a deep CNN to protect CAN or controller area network bus, located inside a vehicle in vehicular networks. The deep CNN learns the pattern of the network traffic and recognizes attack traffic with no need for features designed by humans and recognizes message injection attacks according to the traffic changes. This IDS scheme is designed utilizing the Inception-ResNet model designed for image classification while reducing its size and layers. To use the CAN messages as input to the deep CNN classifier, they generated a 2-D data frame like an image with sequential bitwise identifiers of CAN messages. They indicated that their IDS could recognize attack traffics such as DoS, fuzzy attacks, and spoofing attacks. They considered four message injection attacks in their experiments that exploited the CAN bus. This scheme is evaluated against the LSTM, SVM, ANN, k-NN, NB, and decision tree classifiers and the authors indicated that the LSTM and ANN provide better performance but incur more FNR and ER.

Also, in [200], Song *et al.* proposed an IDS solution using CNN to protect the vehicle's controller area network bus. This scheme applies the CNN, provided using the Inception-ResNet model structure presented for image classification, to learn the traffic patterns of the network and detect attack traffic with a high detection rate. However, since the Inception-ResNet architecture is complicated, they restructured the CNN by mitigating its size and layers. They provided a frame builder, a module that produces a 2-D data frame similar to an image with sequential bitwise identifiers of CAN messages and enables the CNN to learn input data temporal patterns. They constructed fully labeled datasets for the attacks of the in-vehicle network by injecting the CAN messages. By performing the required experiments they demonstrated that their IDS can have low false-negative rates and error rates, comparing to other machine learning methods. Nonetheless, the proposed CNN model cannot handle new attacks.

Also, Bu *et al.* [201], proposed CN-LCS, an IDS approach for a relational database management system that uses CNN and LCS or Learning Classifier System. This scheme can classify sparse and high-dimensional feature vectors of database queries with convolution-pooling operations and GA-based feature selection. Furthermore, in this scheme, CNN is used to classify the queries by modeling normal behaviors of the database, and the GA-based LCS is used to find new rules for detecting anomalies. The authors performed the necessary experiments on the TPC-E dataset and showed that their scheme presents better accuracy than other machine learning methods. However, further evaluation of the proposed scheme seems to be necessary, and also the authors failed to further tune the genetic operators applied in the CN-LCS for ensuring stable performance.

In [202], Li *et al.* proposed DeepFed, a federated deep learning-based IDS scheme for detecting security threats by using the CNN and gated recurrent unit. They introduced a federated learning framework for creating IDS using data from multiple systems. Also, they used a Paillier public key-based cryptography system for securing the proposed model in the training process. The authors run the experiments using a real dataset for industrial cyber-physical systems and demonstrated the effectiveness of their approach. However, DeepFed does not address the cyber-security problems from different-domain cyber-physical systems.

The IDS scheme proposed in [203], applies the CNN to detect DoS attacks in a hybrid network-based IDS and it consists of four convolutional layers, two pool layers, three dropout layers, two dense layers, one flatten layer, and one softmax layer. For evaluation of this IDS approach, Wireshark and Weka tools are employed and datasets such as ISCXIDS 2012 and NSL-KDD are used. The authors indicated that by using the CNN their scheme can achieve higher accuracy than other machine learning algorithms.

Riyaz *et al.* [204], provided an IDS scheme for wireless networks, which uses CRF-LCFS, a feature selection method that applies linear correlation coefficient and conditional random field. This feature selection method applies the conditional random field for choosing variables used in the feature selection using correlation coefficient variance. The proposed feature selection approach provides important features for the CNN that is used for the classification step. At last, the author exhibited that their model achieves less false alarm rate, training, and testing time while getting high detection accuracy compared with the other CNN-based IDS schemes. Also, in [205], Wu *et al.* presented a NIDS model utilizing CNNs, in which the CNN is incorporated for automatically selecting features from raw network traffic. To process data with CNN, this scheme converts the raw network traffic vector into the two-dimensional image format. They set the cost function weight coefficient of each class based on its numbers to solve the imbalanced data set problem. They used the NSL-KDD dataset for evaluating their CNN model's performance and showed that it has lower computational complexity while achieving better results in terms of accuracy and FAR. Table 8 indicates the evaluation metrics, tools, feature extractions, and datasets applied in the CNN-based intrusion detection schemes.

G. HYBRID IDS SCHEMES

In [206], Xu *et al.* introduced LCVAE, a deep learning-based IDS method using a log-cosh conditional variational auto-encoder, which can capture the observed data distribution and can provide new data in the specific classes. In this scheme, the authors the log hyperbolic cosine function to introduce a loss term, which can balance the generation procedures and generates different data for classes that are imbalanced. Besides, they utilized the CNN-based classification based on the observed and generated intrusion. Finally, they conducted the required experiments using NSL-KDD and demonstrated their scheme capabilities in generating new diverse intrusion data.

Yang *et al.* [207], proposed ICVAE-DNN, an IDS model that combines an improved conditional variational auto-encoder with a DNN. In this scheme, the auto-encoder is used to learn and explore sparse representations between network data features and classes. The trained ICVAE decoder generates new attack samples according to the specified intrusion categories to balance the training data and increase the diversity of training samples, improving the detection rate of the imbalanced attacks. The trained ICVAE encoder is not only used to automatically reduce data dimension but initialize the weight of DNN hidden layers so that DNN can easily achieve global optimization through backpropagation and fine-tuning. The authors used the NSL-KDD and UNSW-NB15 datasets are used for evaluating their scheme and indicated that their scheme can outperform other IDS approaches regarding metrics such as accuracy, detection rate, and false-positive rate, even detecting minority attacks and unknown attacks.

In [208], Hara *et al.* introduced an IDS scheme that employs semi-supervised learning which uses a small number of labeled data in the training dataset to reduce costly human-labor tasks and improves the performance with the support of unlabeled data in the training dataset. This scheme uses the adversarial auto-encoder, a semi-supervised learning algorithm that incorporates the GAN into the auto-encoder. They evaluated their approach using the NSL-KDD dataset and indicated that their scheme by using only 0.1 percent of labeled data achieves comparable performance with existing IDSs that use machine learning methods.

In [209], Zhang *et al.* introduced Tiki-Taka, a deep learning-based NIDS approach for handling security attacks. They trained MLP, CNN, and C-LSTM models on the CSE-CIC-IDS2018 dataset and employed 5 categories of security attacks. This scheme provides query detection, ensembling adversarial training, and model voting ensembling. The authors compared their scheme against MLP, CNN, and C-LSTM-based IDS approaches with metrics such as precision, accuracy, Recall, and F1-Score. They exhibited that although their models have high detection rates, it is vulnerable to adversarial samples.

IV. DISCUSSION

This section intends to compare the various techniques and methods employed in intrusion detection schemes. The results of this section can be useful in highlighting the directions of future researches. This section provides the following information about these schemes:

- Simulation metrics used in the evaluation of the studied intrusion detection solutions.
- Environments, programming languages, and simulator software appealed to verify the proposed intrusion detection schemes.
- Datasets used to evaluate and assess deep learning-based intrusion detection solutions.
- The applied feature extraction methods.
- The number of intrusion detection schemes designed using each type of deep learning technique.
- The publication year of the investigated intrusion detection frameworks.
- Accuracy of the deep IDS schemes on several open datasets such as KDDCup, NSL-KDD, ISCX, and UNSW-NB15.

Figure 5 exhibits some of the evaluation metrics employed by the deep learning-based intrusion detection schemes and the number of systems that have utilized each factor in their experiments to verify their results. As shown in this figure, metrics such as accuracy, precision, and recall are widely used by the studied intrusion detection approaches.

Figure 6 indicates the percentage of the different feature extraction methods in the investigated deep learning-based IDS schemes. As shown in this figure, feature extraction methods such as entropy and PCA are widely utilized by the outlined IDS schemes. Likewise, Figure 7 specifies the percentage of the simulators applied in the analyzed

TABLE 8. Comparison of the CNN-based intrusion detection approaches.

	Evaluation metrics											Simulators/Tools/Programming Languages					Datasets				
scheme	False Negative	False Positive	True Negative	True Positive	Accuracy	Precision	Recall	F-measure	Error	Detection Rate	False Alarm Rate	MATLAB	Snort	TensorFlow	Python	Java	KDDCup99	NSL-KDD	DARPA	ISCX	Self-Collected
[162]	✓	✓	✓	✓	✓	✓	✓	✓						✓			✓				
[205]	✓	✓	✓	✓	✓					✓	✓	✓						✓			
[163]					✓										✓						✓
[164]						✓	✓	✓						✓				✓			
[165]	✓	✓	✓	✓	✓										✓					✓	
[166]					✓							✓					✓				
[167]															✓			✓			
[190]					✓					✓	✓			✓			✓				
[191]	✓	✓	✓	✓		✓	✓	✓			✓	✓						✓			
[192]					✓	✓	✓					✓								✓	
[193]														✓							✓
[194]					✓	✓	✓	✓													
[195]					✓							✓					✓	✓			
[196]																					✓
[197]						✓	✓							✓						✓	
[198]														✓							✓
[199]						✓	✓					✓									✓
[200]		✓							✓		✓			✓							✓
[201]		✓				✓		✓							✓		✓				
[202]					✓		✓	✓		✓				✓			✓				
[203]						✓		✓		✓	✓							✓			✓
[204]	✓				✓				✓					✓				✓			
[205]					✓		✓	✓		✓	✓				✓						
[190]	✓	✓	✓			✓				✓							✓	✓			
[206]	✓		✓		✓		✓		✓		✓	✓							✓		
[207]		✓				✓	✓			✓				✓				✓			
[208]	✓					✓		✓		✓					✓				✓		✓
[209]							✓			✓		✓					✓				

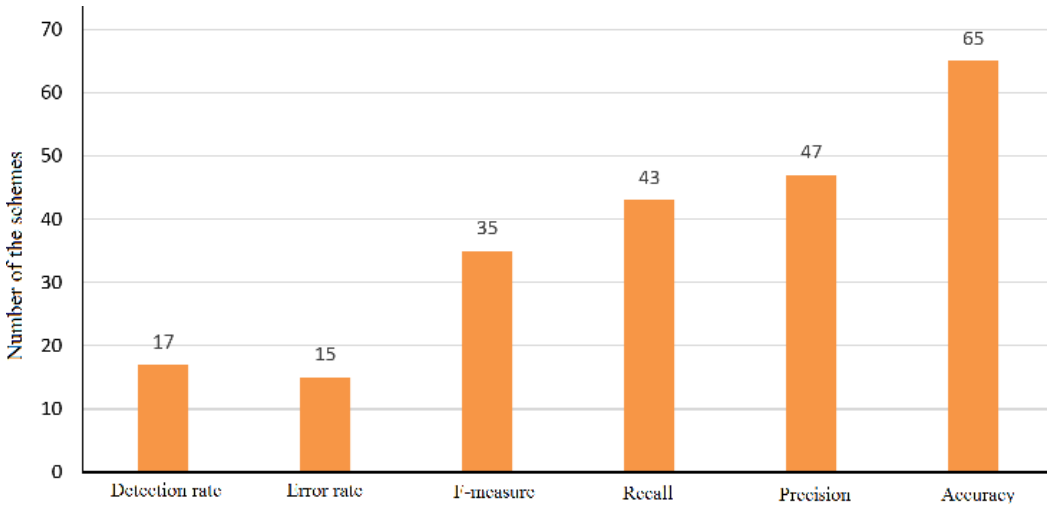


FIGURE 5. Number of the deep learning-based schemes applied to each evaluation factor.

systems to evaluate their performance and indicate their advantages. It exhibits that the outlined deep learning-based IDS approaches have mostly used the TensorFlow simulator and python programming language in their experiments. TensorFlow is an open-source software tool implemented by Google for operating systems like Mac, Linux, Android, iOS,

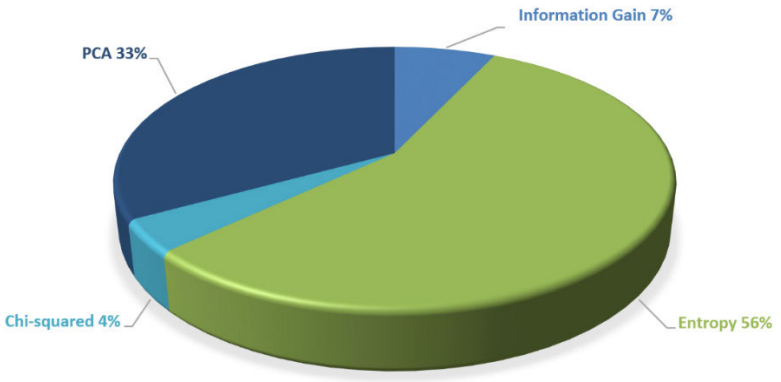


FIGURE 6. Percentage of the feature extraction methods.

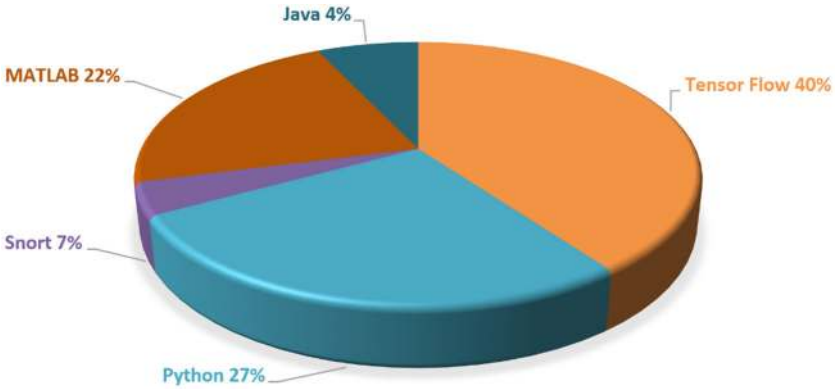


FIGURE 7. The simulators and software tools.

and Windows. It can be applied to data flow graphs and differentiable programming. It is employed in applications such as ANNs and can operate on several GPUs and CPUs. It also introduces various levels of distributed and parallel operations.

Another environment that is applied by some of the deep IDS schemes is Snort, which is a free and open-source IDS tool that can be used on small networks. It can be run on operating systems such as BSD, Linux, Windows, and Mac. Furthermore, Snort doesn't need to recompile the kernel and does not need specific hardware or software. In addition to the before-mentioned environments, recently other software tools such as DeepLearning4j, Caffe, Torch, Theano, MXNet, Neon, and Microsoft Cognitive Toolkit can be used for designing deep learning-based solutions. Figure 8 exhibits the datasets applied in the investigated approaches and determines the number of schemes that have employed each type of dataset. It can be concluded from this figure, the primary datasets used in this context are the NSLKDD and KDD-Cup99, which are pretty old. Likewise, the other datasets shown in this figure can be described as follows:

- UNSW-NB15 dataset contains 42 features, and 32% of its records are normal, and 68% of its records are malicious.
- CIDDS-001 dataset is a flow-based one that consists of 10 features and five classes: unknown, attacker, suspicious, normal, and victim. It can be applied to evaluate the IDS approaches and consists of malicious traffics such as DDoS, brute force, and port scans.
- GPRS is a dataset designed for IEEE 802.11 environments and has 15 features for two different topologies: WEP/WPA and WPA2.

Figure 9 depicts the number of intrusion detection schemes designed using each type of deep learning technique. This figure indicates that more IDS schemes favor deep neural networks such as auto-encoders, DNN, and CNN.

The percentage of the intrusion detection schemes which have applied raw data or existing benchmark IDS datasets in their experiments and evaluations are shown in Figure 10. As shown in this figure, most of the schemes have assumed that the required data for training and testing are pre-stored in the datasets and only use them. Such systems often consider that no other data will be added to the dataset, and there is no need for incremental training of classifiers. Also, a few numbers of the investigated IDS schemes have focused on the processing of the raw data achieved from monitoring the streaming network traffic or host events. These schemes often use incremental learning, which uses input data for continuous training of the IDS model and extracting new security attack signatures. Another item that we illuminate about the studied schemes is their accuracy.

For this purpose, Figure 11 compares the accuracy of the several deep IDS schemes, which the authors have claimed achieved on their experiment conducted on the KDDCup

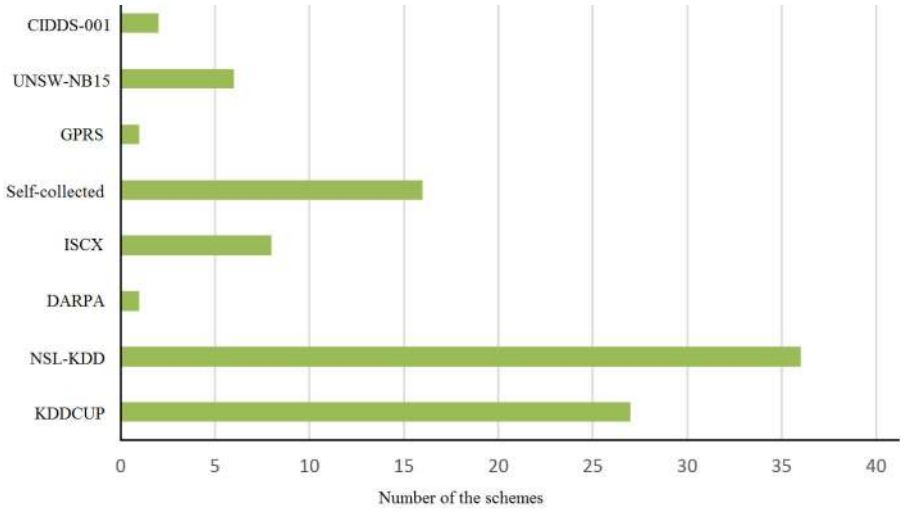


FIGURE 8. Applied datasets.

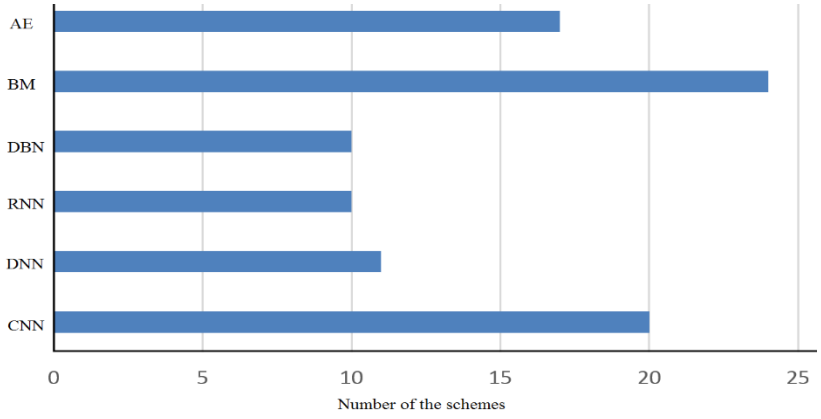


FIGURE 9. Number of IDS schemes designed using each type of deep learning system.

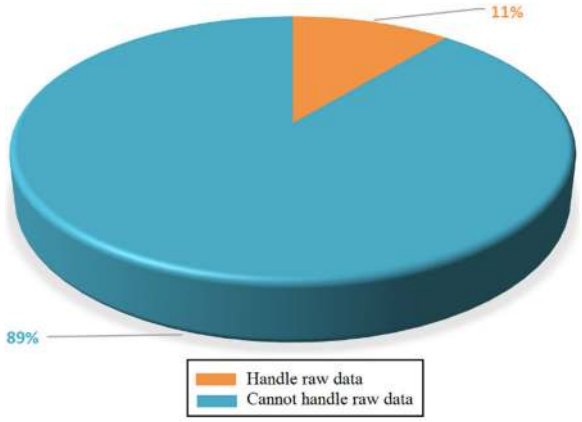


FIGURE 10. Percentage of the schemes applied raw data or existing datasets.

dataset. Also, Figure 12 indicates the accuracy of some other deep IDS schemes on the NSL-KDD dataset. Figure 13 depicts the accuracy of the deep IDS approaches achieved on the ISCX dataset, and Figure 14 indicates the accuracy results achieved on the UNSW-NB15 dataset by some of the deep learning-based IDS solutions. As shown in these figures, fewer schemes have evaluated the newer datasets, and in future studies, verification of the proposed schemes should be evaluated on the newer datasets that better reflect the real traffic of the target environment. Deep learning methods have been used for classification and feature learning purposes, in which the latter method reduces the complexity of the raw features of the dataset. As shown in previous sections, auto-encoders are often used for feature learning, and RNNs are applied for classification purposes. Regarding the need for real-time IDS schemes, the online learning method is applied in some of the studied deep IDS approaches. Also, online learning cannot be easily parallelized, and each input data need a linear learning rate. Also, in online learning, it is assumed that data have a similar distribution and possess a specific amount of correlation. In this learning method, data with time-varying distributions can be a challenging issue.

Consequently, handling such challenges in the online learning and application of the proposed methods in deep IDS schemes should be investigated. As outlined before,

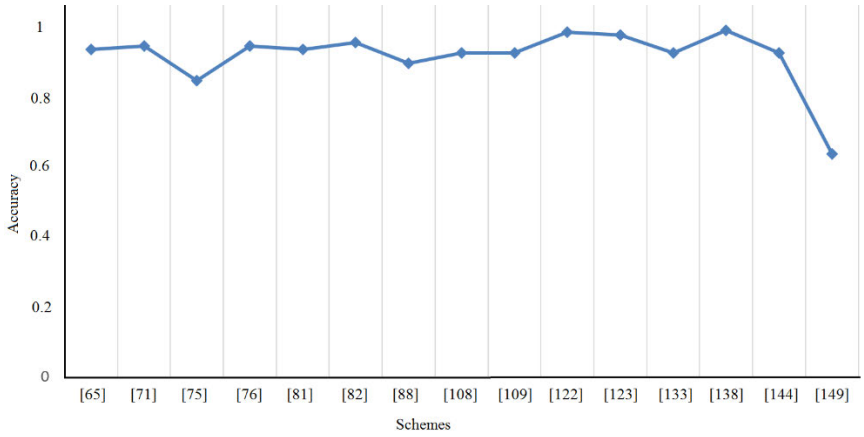


FIGURE 11. Accuracy of the KDDCup-based deep IDS schemes.

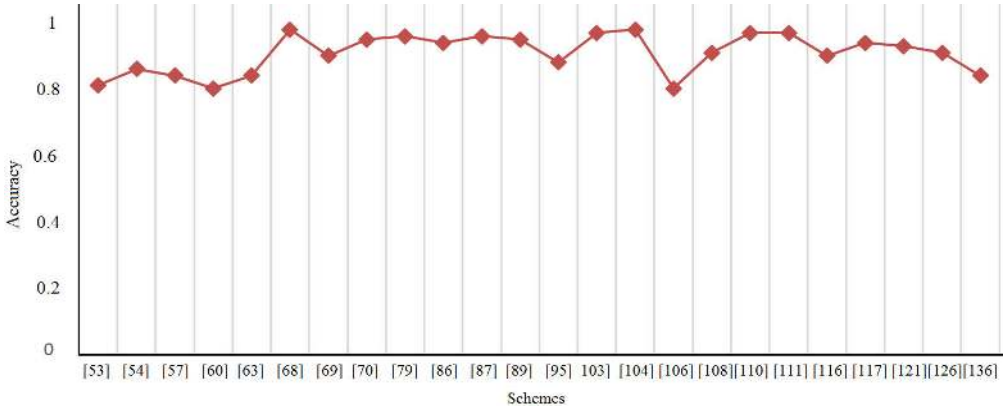


FIGURE 12. Accuracy of the NSL-KDD-based deep IDS schemes.

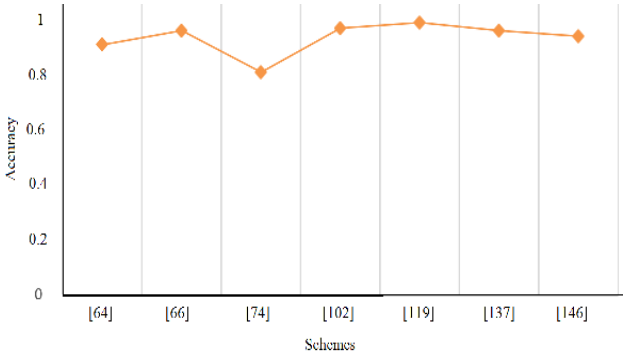


FIGURE 13. Accuracy of the ISCX-based deep IDS schemes.

FIGURE 14. Accuracy of the UNSW-NB15-based deep IDS schemes.

in some of the studied schemes, deep learning in some IDS schemes has been used for feature selection/extraction. In such schemes, improved versions of the machine learning algorithms can be further used to increase the performance of the intrusion detection process. The training of deep learning networks is another interesting issue that is aimed at finding the network parameters for minimizing the loss function. Currently, for the training of the deep networks, the SGD or Stochastic Gradient Descent algorithm is used to tune the network parameters based on the gradient for each training sample. Typically, the SGD's complexity is less than the basic gradient descent method, and in its learning phase, the learning rate hyper-parameter tunes the updating speed. Numerous methods are proposed for accelerating the convergence and determining the learning rate. In the subsequent studies, tuning the SGD's learning rate can be investigated further. Furthermore, by the conducted investigations, it can be

TABLE 9. Challenges, issues and future works in the deep learning-based misuse detection.

Index	Issue
1	Recently several new DoS attacks are introduced against different layers of computer networks, but most of the studied intrusion detection approaches are analyzed with the older datasets such as KDDCup99. Thus, creating new datasets containing various DoS attacks' signatures and further evaluations with them is of high importance.
2	Since there are fewer records for attacks like R2L and U2R in the DARPA-based datasets, it is difficult for classifiers to detect them. Regardless of such problems in datasets, the proposed IDS schemes should handle imbalanced datasets by various means. For instance, the auto-encoder can handle imbalanced classification problems and can deal with both minority and majority classes. Also, in this context, evaluation of the other datasets which have imbalanced classes can be useful in the verification of the detection rate of the attack classes.
3	Using the newly proposed optimization algorithms for efficient training of the various deep neural networks can also be investigated in future studies. Training deep networks using optimization algorithms for intrusion detection can be an interesting issue to focus on in the next studies.
4	Most of the studied schemes have applied pre-existed datasets for evaluation of their scheme; however, as outlined before, it is ideal for a network IDS to extract its essential features from raw bytes of network traffic instead of using existing features from datasets. Although few schemes have been presented with the raw data processing capability, further studies are required in this context.
5	The application of the online learning approach, in combination with deep neural network-based intrusion detection frameworks, can be studied in the future.
6	Other shallow learning methods should be analyzed in the performance evaluation of the proposed schemes to evaluate intrusion detection performance.
7	As was discussed in the previous section, only some of the shallow learning methods are applied in combination with the deep learning methods. Thus, in future studies, the performance of other classifiers can be further investigated, in combination with deep learning-based techniques.
8	Recently, GPUs are designed for handling the execution of complicated operations. It can be useful to analyze the training and execution time of the proposed intrusion detection schemes in terms of learning time and testing time by conducting experiments on the multi-core CPUs and GPUs.
9	Only a few numbers of deep IDS schemes are introduced for vehicular networks, IoT, and E-healthcare systems. Thus, in the future, the performance of the deep neural network-based IDS schemes should be further investigated in these contexts.
10	Typically, most existing investigations and implementations of the deep learning schemes are conducted using supervised learning methods that apply large labeled datasets. However, in some cases, the existing datasets are not large enough to train deep models, or there is no dataset to train the deep models, and the required data should be handled in real-time without any labeling data. In such cases, instead of supervised learning, other learning methods such as unsupervised and semi-supervised learning techniques should be used. However, only a handful of investigated IDS schemes have incorporated unsupervised learning and semi-supervised learning techniques, and in the future, these learning methods should be further explored.
11	Typically, deep learning cannot easily model several complex data modalities. Thus, in the subsequent studies, deep multimodal learning should be further investigated. Besides, deep learning-based multimodal intrusion detection has been discussed by a few schemes, and it should also be addressed in the future.
12	Other implementations of the deep learning techniques such as parallel and distributed deep learning models are not applied in the studied intrusion detection frameworks and can be focused on the next studies conducted, which can be conducted to build large IDS.
13	Another critical issue in the deep learning-based intrusion detection approaches is to conduct the training process on massive datasets. In this context, the extremely long training time of the deep learning models remains a significant problem for researchers. Thus, improving the training speed of the deep IDS schemes should be studied in the subsequent investigations.

concluded that few deep IDS schemes are proposed for environments such as VANETs, Internet of Things (IoT), mobile edge computing, software-defined network, and healthcare systems, and it has not been well-studied in these domains. Thus, introducing special-purpose deep IDS approaches for such environments should be further studied in the next IDS studies. Besides, in such schemes, using datasets that reflect the inherent traffic of the environment is of the main issues. In this context, some of the schemes, such as [150], have produced their required datasets by capturing traffic from their environments, and some others, such as [197], have used simulated traffics. Besides, in designing deep IDS approaches, high resource consumption of the deep learning techniques should be considered, especially in domains such as IoT, which consists of many resource-limited devices.

From the results of the previous section, it can be seen that most of the schemes have used the KDDCup-based datasets, which are old and cannot represent the current threats and security attacks. Thus, due to the limitations of the existing datasets, creating new datasets in the IDS context and different domains should enable proper verification of the newly proposed IDS schemes.

Based on the type of traffic which the studied IDS schemes can handle, the proposed schemes can be classified as the schemes which handle unencrypted traffic and schemes that are designed to deal with encrypted traffics. Nonetheless, only a handful of schemes have been designed to detect intrusion on encrypted traffic. Thus, further studies on encrypted traffic seem to be necessary for different domains.

Typically, the deep learning techniques have high computational needs, and their training latency and computation complexity raise according to the number of their applied neurons and layers. Furthermore, when a deep IDS scheme uses a large dataset, techniques such as cross-validation, which are used to reduce the over-fitting problem, can incur further training costs. Several approaches are proposed approach in the literature to deal with this issue; for instance, reservoir computing, hardware-assisted methods, and incremental methods are used in offline training. Furthermore, cloud computing processing capabilities can be benefited in some domains, such as the IoT, to reduce the deep learning overheads. From the studied deep IDS schemes, mostly applied GPU to increase the performance of the learning process. But, GPUs suffer from the current leakage problem, and this prevents its application on portable devices. Although FPGA or Field-Programmable Gate Arrays are used to deal with this problem, finding other solutions to increase the performance of deep network training should be studied to increase the training speed of the deep techniques.

One of the interesting solutions to deal with the training speed of the deep learning methods is distributed deep learning. In this context, model parallelism and data parallelism methods are proposed for training the deep model in a distributed system, in which for model parallelism, all data should be handled with one model, and all nodes participate in estimating the model's parameters. Also, in data parallelism methods, the deep model should be replicated on all the nodes to be trained with a part of the dataset, and nodes cooperate to update and synchronize the model weights. Using distributed deep learning techniques can further enhance the training speed of the deep learning-based intrusion detection process and should be analyzed in subsequent researches.

Another interesting method that is used for reducing the training time of deep learning networks is transfer learning that for small new datasets can be performed with the pre-trained networks as fixed feature extractors, and for large new datasets, can be conducted using fine-tuning the weights of the pre-trained model. In the forthcoming IDS approaches, transfer learning can be further investigated to enhance the intrusion detection process. Table 9 indicates the future research directions in the deep learning-based intrusion detection domain.

V. CONCLUSION

Intrusion detection systems are one of the essential security components of the current information technology-based organizations. However, providing an efficient and high-performance IDS approach to deal with a wide variety of security attacks is a challenging approach. Recently, deep learning techniques have proved to deal with intrusion detection problems, and several deep learning-based IDS schemes are introduced in the literature. Deep learning is a subset of machine learning techniques, which incorporate several layers to conduct nonlinear processing and learn several data representation levels. Deep learning networks can process raw input data and support unsupervised, semi-supervised, and supervised learning methods.

This article provides an in-depth review and classification of the intrusion detection schemes which have benefited deep neural networks to deal with intrusions and malicious behaviors. For this purpose, it first categorizes the deep IDS schemes according to their incorporated deep learning techniques and describes how each scheme is trying to apply deep learning methods for recognizing various types of intrusions. Besides, in the studied deep IDS schemes, the shallow learning methods utilized in combination with the deep learning techniques are investigated. Moreover, to provide an in-depth insight into the studied IDS frameworks, in each category of the studied approaches, their primary contributions, advantages, and limitations are specified. Besides, in each category, their utilized evaluation metrics, simulators, and datasets are compared. At last, it can be concluded that deep learning is an interesting method, which puts forward many opportunities and also challenges in the intrusion detection context.

REFERENCES

[1] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3724–3751, Nov. 2016.

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, Mar. 2013.

[3] M. Masdari, S. Ahmadzadeh, and M. Bidaki, "Key management in wireless body area network: Challenges and issues," *J. Netw. Comput. Appl.*, vol. 91, pp. 36–51, Aug. 2017.

[4] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: Analysis and open research issues," *Wireless Netw.*, vol. 20, no. 8, pp. 2165–2199, 2014.

[5] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016.

[6] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, Jun. 2017.

[7] Y. Sun, F. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[8] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced Internet of Things for personalised healthcare systems: A survey," *Pervasive Mobile Comput.*, vol. 41, pp. 132–149, Oct. 2017.

[9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, 2012, pp. 13–16.

[10] M. Masdari and A. Khoshnevis, "A survey and classification of the workload forecasting methods in cloud computing," *Cluster Comput.*, vol. 23, no. 4, pp. 2399–2424, Dec. 2020.

[11] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, and K.-K. R. Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, Oct. 2016.

[12] M. Masdari, S. M. Bazarchi, and M. Bidaki, "Analysis of secure LEACH-based clustering protocols in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 4, pp. 1243–1260, Jul. 2013.

[13] M. Premkumar and T. V. P. Sundararajan, "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks," *Microprocessors Microsyst.*, vol. 79, Nov. 2020, Art. no. 103278.
[14] M. Masdari, S. Jabbehdari, M. R. Ahmadi, S. M. Hashemi, J. Bagherzadeh, and A. Khadem-Zadeh, "A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, no. 1, pp. 1–12, Dec. 2011.
[15] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *J. Syst. Archit.*, vol. 105, May 2020, Art. no. 101701.
[16] M. Masdari, S. Jabbehdari, J. Bagherzadeh, and A. Khadem-Zadeh, "Towards efficient certificate status validations with E-ADOPT in mobile ad hoc networks," *Comput. Secur.*, vol. 49, pp. 17–27, Mar. 2015.
[17] N. Firouz, M. Masdari, A. B. Sangar, and K. Majidzadeh, "A novel controller placement algorithm based on network portioning concept and a hybrid discrete optimization algorithm for multi-controller software-defined networks," *Cluster Comput.*, pp. 1–34, Apr. 2021.
[18] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN Future Netw. Services (SDN FNS)*, Nov. 2013, pp. 1–7.
[19] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," *Cluster Comput.*, vol. 24, pp. 1–19, Jun. 2020.
[20] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013.
[21] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Comput.*, vol. 22, pp. 1–13, Nov. 2017.
[22] D. Moon, S. B. Pan, and I. Kim, "Host-based intrusion detection system for secure human-centric computing," *J. Supercomput.*, vol. 72, no. 7, pp. 2520–2536, Jul. 2016.
[23] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based intrusion detection systems," *Appl. Soft Comput.*, vol. 92, Jul. 2020, Art. no. 106301.
[24] N. Pandeeswari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering based ANN," *Mobile Netw. Appl.*, vol. 21, no. 3, pp. 494–505, Jun. 2016.
[25] M. Masdari and H. Khezri, "Towards fuzzy anomaly detection-based security: A comprehensive review," *Fuzzy Optim. Decis. Making*, vol. 20, no. 1, pp. 1–49, Mar. 2021.
[26] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Comput. Commun.*, vol. 49, pp. 1–17, Aug. 2014.
[27] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "Security anomaly detection in software-defined networking based on a prediction technique," *Int. J. Commun. Syst.*, vol. 33, no. 14, p. e4524, Sep. 2020.
[28] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "SADM-SDNC: Security anomaly detection and mitigation in software-defined networking using C-support vector classification," *Computing*, vol. 103, no. 4, pp. 641–673, Apr. 2021.
[29] G. Pang, C. Shen, L. Cao, and A. Hengel, "Deep learning for anomaly detection: A review," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–38, 2020.
[30] S. Thudumu, P. Branch, J. Jin, and J. Singh, "A comprehensive survey of anomaly detection techniques for high dimensional big data," *J. Big Data*, vol. 7, no. 1, pp. 1–30, Dec. 2020.
[31] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.
[32] R. Yan, X. Xiao, G. Hu, S. Peng, and Y. Jiang, "New deep learning method to detect code injection attacks on hybrid applications," *J. Syst. Softw.*, vol. 137, pp. 67–77, Mar. 2018.
[33] M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri, and M. M. Hassan, "A prediction system of sybil attack in social network using deep-regression model," *Future Gener. Comput. Syst.*, vol. 87, pp. 743–753, Oct. 2018.
[34] H. Shi, H. Li, D. Zhang, C. Cheng, and X. Cao, "An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification," *Comput. Netw.*, vol. 132, pp. 81–98, Feb. 2018.
[35] A. Prieto, B. Prieto, E. M. Ortigosa, E. Ros, F. Pelayo, J. Ortega, and I. Rojas, "Neural networks: An overview of early research, current frameworks and new challenges," *Neurocomputing*, vol. 214, pp. 242–268, Nov. 2016.
[36] A. Aleesa, B. Zaidan, A. Zaidan, and N. M. Sahar, "Review of intrusion detection systems based on deep learning techniques: Coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," *Neural Comput. Appl.*, vol. 32, pp. 1–32, Jul. 2020.
[37] (2017). *McAfee Labs Threat Report*. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sept-2017.pdf
[38] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "A survey on deep learning for big data," *Inf. Fusion*, vol. 42, pp. 146–157, Jul. 2018.
[39] S. Osken, E. N. Yildirim, G. Karatas, and L. Cuhaci, "Intrusion detection systems with deep learning: A systematic mapping study," in *Proc. Sci. Meeting Elect.-Electron. Biomed. Eng. Comput. Sci. (EBBT)*, Apr. 2019, pp. 1–4.
[40] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, Feb. 2020, Art. no. 105124.
[41] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019.
[42] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "A comparative analysis of deep learning approaches for network intrusion detection systems (N-IDSs): Deep learning for N-IDSs," *Int. J. Digit. Crime Forensics*, vol. 11, no. 3, pp. 65–89, Jul. 2019.
[43] G. Litjens, T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. A. Van Der Laak, B. Van Ginneken, and C. I. Sánchez, "A survey on deep learning in medical image analysis," *Med. Image Anal.*, vol. 42, pp. 60–88, Dec. 2017.
[44] L. Zhang, S. Wang, and B. Liu, "Deep learning for sentiment analysis: A survey," *Wiley Interdiscipl. Rev., Data Mining Knowl. Discovery*, vol. 8, p. e1253, Jul. 2018.
[45] S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep learning based recommender system: A survey and new perspectives," *ACM Comput. Surveys*, vol. 52, no. 1, pp. 1–38, Feb. 2019.
[46] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2224–2287, 3rd Quart., 2019.
[47] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016.
[48] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.
[49] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Comput. Secur.*, vol. 29, no. 1, pp. 124–140, 2010.
[50] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, p. 55, 2014.
[51] R. Zuech, T. M. Khoshgoftaar, and R. Wald, "Intrusion detection and big heterogeneous data: A survey," *J. Big Data*, vol. 2, no. 1, p. 3, Dec. 2015.
[52] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Comput. Surv.*, vol. 47, no. 4, p. 55, Jul. 2015.
[53] H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020.
[54] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," 2017, *arXiv:1701.02145*. [Online]. Available: http://arxiv.org/abs/1701.02145
[55] M. Masdari, "Markov chain-based evaluation of the certificate status validations in hybrid MANETs," *J. Netw. Comput. Appl.*, vol. 80, pp. 79–89, Feb. 2017.
[56] J. Yan, D. Jin, C. W. Lee, and P. Liu, "A comparative study of off-line deep learning based network intrusion detection," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 299–304.
[57] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019.

[58] S. Parampottupadam and A.-N. Moldovann, "Cloud-based real-time network intrusion detection using deep learning," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Security)*, Jun. 2018, pp. 1–8.

[59] H. A. Najada, I. Mahgoub, and I. Mohammed, "Cyber intrusion prediction and taxonomy system using deep learning and distributed big data processing," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2018, pp. 631–638.

[60] G. Karatas, O. Demir, and O. K. Sahingoz, "Deep learning in intrusion detection systems," in *Proc. Int. Congr. Big Data, Deep Learn. Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018, pp. 113–116.

[61] A. Anzer and M. Elhadef, "Deep learning-based intrusion detection systems for intelligent vehicular ad hoc networks," in *Advanced Multimedia and Ubiquitous Engineering*. Springer, 2018, pp. 109–116.

[62] Z. Wang, "Deep learning-based intrusion detection with adversaries," *IEEE Access*, vol. 6, pp. 38367–38384, 2018.

[63] N. Chockwanich and V. Visoottiviseth, "Intrusion detection by deep learning with TensorFlow," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 654–659.

[64] S. Wang, B. Li, M. Yang, and Z. Yan, "Intrusion detection for WiFi network: A deep learning approach," in *Proc. Int. Wireless Internet Conf.*, 2018, pp. 95–104.

[65] L. Gao, F. Li, X. Xu, and Y. Liu, "Intrusion detection system using SOEKS and deep learning for in-vehicle security," *Cluster Comput.*, vol. 22, pp. 1–9, Nov. 2018.

[66] S. Ustebay, Z. Turgut, and M. A. Aydin, "Intrusion detection system with recursive feature elimination by using random forest and deep learning classifier," in *Proc. Int. Congr. Big Data, Deep Learn. Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018, pp. 71–76.

[67] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[68] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101974.

[69] T.-N. Dao and H. J. Lee, "Stacked autoencoder-based probabilistic feature extraction for on-device network intrusion detection," *IEEE Internet Things J.*, early access, May 7, 2021, doi: 10.1109/JIOT.2021.3078292.

[70] A. Abusitta, M. Bellaiche, M. Dagenais, and T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Future Gener. Comput. Syst.*, vol. 98, pp. 308–318, Sep. 2019.

[71] H. Zhang, C. Q. Wu, S. Gao, Z. Wang, Y. Xu, and Y. Liu, "An effective deep learning based scheme for network intrusion detection," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 682–687.

[72] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019.

[73] C. Ieracitano, A. Adeel, M. Gogate, K. Dashtipour, F. C. Morabito, H. Larijani, A. Raza, and A. Hussain, "Statistical analysis driven optimized deep learning system for intrusion detection," in *Proc. Int. Conf. Brain Inspired Cognit. Syst.*, 2018, pp. 759–769.

[74] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, *arXiv:1802.09089*. [Online]. Available: http://arxiv.org/abs/1802.09089

[75] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS)*, 2016, pp. 21–26.

[76] M. Ishaque and L. Hudec, "Feature extraction using deep learning for intrusion detection system," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–5.

[77] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning," *Int. J. Inf. Secur.*, vol. 20, pp. 1–17, Jun. 2020.

[78] C. Zhang, F. Ruan, L. Yin, X. Chen, L. Zhai, and F. Liu, "A deep learning approach for network intrusion detection based on NSL-KDD dataset," in *Proc. IEEE 13th Int. Conf. Anti-Counterfeiting, Secur., Identificat. (ASID)*, Oct. 2019, pp. 41–45.

[79] Y. Liu, Q. Liao, J. Zhao, and Z. Han, "Deep learning based encryption policy intrusion detection using commodity WiFi," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2019, pp. 2129–2135.

[80] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," *Comput. Electr. Eng.*, vol. 91, May 2021, Art. no. 107044.

[81] R. Zhao, J. Yin, Z. Xue, G. Gui, B. Adebisi, T. Ohtsuki, H. Gacanin, and H. Sari, "An efficient intrusion detection method based on dynamic autoencoder," *IEEE Wireless Commun. Lett.*, early access, May 6, 2021, doi: 10.1109/LWC.2021.3077946.

[82] A. Basati and M. M. Faghih, "APAE: An IoT intrusion detection system using asymmetric parallel auto-encoder," *Neural Comput. Appl.*, pp. 1–21, Apr. 2021.

[83] W. Xu, Y. Fan, and C. Li, "I2DS: Interpretable intrusion detection system using autoencoder and additive tree," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Mar. 2021.

[84] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018.

[85] S. N. Mighan and M. Kahani, "Deep learning based latent feature extraction for intrusion detection," in *Proc. Electr. Eng. (ICEE), Iranian Conf.*, May 2018, pp. 1511–1516.

[86] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 178–183.

[87] Y. Yu, J. Long, and Z. Cai, "Session-based network intrusion detection using a deep learning architecture," in *Modeling Decisions for Artificial Intelligence*. Cham, Switzerland: Springer, 2017, pp. 144–155.

[88] Q. Niyaz, W. Sun, and A. Y Javaid, "A deep learning based DDoS detection system in software-defined networking (SDN)," 2016, *arXiv:1611.07400*. [Online]. Available: http://arxiv.org/abs/1611.07400

[89] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 169–175, Feb. 2018.

[90] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.

[91] P. V. Dinh, T. N. Ngoc, N. Shone, A. MacDermott, and Q. Shi, "Deep learning combined with de-noising data for network intrusion detection," in *Proc. 21st Asia Pacific Symp. Intell. Evol. Syst. (IES)*, 2017, pp. 55–60.

[92] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security on neuromorphic computing system," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, 2017, pp. 3830–3837.

[93] C. Kim and J. Park, "Designing online network intrusion detection using deep auto-encoder Q-learning," *Comput. Electr. Eng.*, vol. 79, Oct. 2019, Art. no. 106460.

[94] A. S. Qureshi, A. Khan, N. Shamim, and M. H. Durad, "Intrusion detection using deep sparse auto-encoder and self-taught learning," *Neural Comput. Appl.*, vol. 32, pp. 1–13, Apr. 2020.

[95] F. Louati and F. B. Ktata, "A deep learning-based multi-agent system for intrusion detection," *Social Netw. Appl. Sci.*, vol. 2, no. 4, pp. 1–13, Apr. 2020.

[96] P.-J. Chuang and D.-Y. Wu, "Applying deep learning to balancing network intrusion detection datasets," in *Proc. IEEE 11th Int. Conf. Adv. Infocomm Technol. (ICAIT)*, Oct. 2019, pp. 213–217.

[97] J. Yang, J. Deng, S. Li, and Y. Hao, "Improved traffic detection with support vector machine based on restricted Boltzmann machine," *Soft Comput.*, vol. 21, no. 11, pp. 3101–3112, 2017.

[98] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 68–71, Jun. 2019.

[99] H. Yang, G. Qin, and L. Ye, "Combined wireless network intrusion detection model based on deep learning," *IEEE Access*, vol. 7, pp. 82624–82632, 2019.

[100] A. Elsaeidy, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Intrusion detection in smart cities using restricted Boltzmann machines," *J. Netw. Comput. Appl.*, vol. 135, pp. 76–83, Jun. 2019.

[101] X. Zhang and J. Chen, "Deep learning based intelligent intrusion detection," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 1133–1137.

[102] A. Gouveia and M. Correia, "A systematic approach for the application of restricted Boltzmann machines in network intrusion detection," in *Proc. Int. Work-Conf. Artif. Neural Netw.*, 2017, pp. 432–446.

[103] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security using unsupervised deep learning approaches," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jun. 2017, pp. 63–69.

[104] W. Peng, X. Kong, G. Peng, X. Li, and Z. Wang, "Network intrusion detection based on deep learning," in *Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE)*, 2019, pp. 431–435.

[105] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment," *J. Ambient Intell. Humanized Comput.*, vol. 12, pp. 1–11, Mar. 2019.
[106] P. Wang, X. Song, Z. Deng, H. Xie, and C. Wang, "An improved deep learning based intrusion detection method," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2019, pp. 2092–2096.
[107] Q. Tian, D. Han, K.-C. Li, X. Liu, L. Duan, and A. Castiglione, "An intrusion detection approach based on improved deep belief network," *Appl. Intell.*, vol. 50, pp. 3162–3178, May 2020.
[108] Y. Wu, W. W. Lee, Z. Xu, and M. Ni, "Large-scale and robust intrusion detection model combining improved deep belief network with feature-weighted SVM," *IEEE Access*, vol. 8, pp. 98600–98611, 2020.
[109] C. T. Thanh, "A novel approach for intrusion detection based on deep belief network," in *Proc. Comput. Sci. Conf.*, 2020, pp. 297–311.
[110] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," *Processes*, vol. 9, no. 5, p. 834, May 2021.
[111] W. Wen, C. Shang, Z. Dong, H.-C. Keh, and D. S. Roy, "An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 36, no. 1, pp. 20–31, 2021.
[112] S. Dilipkumar and M. Durairaj, "Epilson swarm optimized cluster gradient and deep belief classifier for multi-attack intrusion detection in MANET," *J. Ambient Intell. Humanized Comput.*, pp. 1–16, Apr. 2021.
[113] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, W. Luo, and Y. Wu, "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system," *IEEE Trans. Ind. Informat.*, early access, Jan. 21, 2021, doi: 10.1109/TII.2021.3053304.
[114] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019.
[115] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in *Proc. 2nd Int. Conf. Adv. Cloud Big Data*, Nov. 2014, pp. 247–252.
[116] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *Proc. Nat. Aerosp. Electron. Conf. (NAECON)*, Jun. 2015, pp. 339–344.
[117] J. Tian and P. Li, "An intrusion detection algorithm of dynamic recursive deep belief networks," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, 2017, pp. 180–183.
[118] O. E. David and N. S. Netanyahu, "DeepSign: Deep learning for automatic malware signature generation and classification," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2015, pp. 1–8.
[119] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, "Hybrid intelligent intrusion detection scheme," in *Soft Computing in Industrial Applications*. Springer, 2011, pp. 293–303.
[120] Y. Yang, K. Zheng, C. Wu, X. Niu, and Y. Yang, "Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks," *Appl. Sci.*, vol. 9, no. 2, p. 238, Jan. 2019.
[121] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," *Sensors*, vol. 19, no. 9, p. 1977, Apr. 2019.
[122] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in SDN-based networks," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 202–206.
[123] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," 2017, *arXiv:1710.00811*. [Online]. Available: http://arxiv.org/abs/1710.00811
[124] K. Al Jallad, M. Aljnidi, and M. S. Desouki, "Big data analysis and distributed deep learning for next-generation intrusion detection system optimization," *J. Big Data*, vol. 6, no. 1, p. 88, Dec. 2019.
[125] Y. Lin, J. Wang, Y. Tu, L. Chen, and Z. Dou, "Time-related network intrusion detection model: A deep learning method," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[126] S. Nayyar, S. Arora, and M. Singh, "Recurrent neural network based intrusion detection system," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Jul. 2020, pp. 0136–0140.
[127] C. Yue, L. Wang, D. Wang, R. Duo, and X. Nie, "An ensemble intrusion detection method for train Ethernet consist network based on CNN and RNN," *IEEE Access*, vol. 9, pp. 59527–59539, 2021.
[128] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, "Stacked recurrent neural network for botnet detection in smart homes," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107039.
[129] R. SaiSindhuTheja and G. K. Shyam, "An efficient Metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment," *Appl. Soft Comput.*, vol. 100, Mar. 2021, Art. no. 106997.
[130] B. Roy and H. Cheung, "A deep learning approach for intrusion detection in Internet of Things using bi-directional long short-term memory recurrent neural network," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–6.
[131] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
[132] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.
[133] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.
[134] F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, "Deep learning based multi-channel intelligent attack detection for data security," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 2, pp. 204–212, Apr. 2020.
[135] S. M. Kasongo and Y. Sun, "A deep long short-term memory based classifier for wireless intrusion detection system," *ICT Exp.*, vol. 6, no. 2, pp. 98–103, Jun. 2020.
[136] S. Kaur and M. Singh, "Hybrid intrusion detection and signature generation using deep recurrent neural networks," *Neural Comput. Appl.*, vol. 32, pp. 1–19, Jun. 2020.
[137] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.
[138] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, May 2020, Art. no. 102031.
[139] K. Yang, J. Liu, C. Zhang, and Y. Fang, "Adversarial examples against the deep learning based network intrusion detection systems," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 559–564.
[140] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.
[141] R. K. Vigneswaran, R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–6.
[142] J.-H. Woo, J.-Y. Song, and Y.-J. Choi, "Performance enhancement of deep neural network using feature selection and preprocessing for intrusion detection," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2019, pp. 415–417.
[143] A. Malathi, J. Amudha, and P. Narayana, "A prototype to detect anomalies using machine learning algorithms and deep neural network," in *Computational Vision and Bio Inspired Computing*. Springer, 2018, pp. 1084–1094.
[144] B. Hu, J. Wang, Y. Zhu, and T. Yang, "Dynamic deep forest: An ensemble classification method for network intrusion detection," *Electronics*, vol. 8, no. 9, p. 968, Aug. 2019.
[145] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2016, pp. 258–263.
[146] K. Arora and R. Chauhan, "Improvement in the performance of deep neural network model using learning rate," in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, Apr. 2017, pp. 1–5.
[147] S. McElwee, J. Heaton, J. Fraley, and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 1–5.
[148] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[149] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101752.

[150] K. Amarasinghe and M. Manic, "Improving user trust on deep neural networks based intrusion detection systems," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 3262–3268.

[151] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. Krishna, "A deep learning based artificial neural network approach for intrusion detection," in *Proc. Int. Conf. Math. Comput.*, 2017, pp. 44–53.

[152] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2017, pp. 313–316.

[153] M.-J. Kang and J.-W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[154] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2016, pp. 1–8.

[155] S. A. Ludwig, "Intrusion detection of multiple attack classes using a deep neural net ensemble," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2017, pp. 1–7.

[156] X. Jin, B. Cui, J. Yang, and Z. Cheng, "Payload-based web attack detection using deep neural network," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, 2017, pp. 482–488.

[157] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in *Proc. Australas. Joint Conf. Artif. Intell.*, 2016, pp. 137–149.

[158] B. A. Tama and K.-H. Rhee, "Attack classification analysis of IoT network via deep learning approach," *Res. Briefs Inf. Commun. Technol. Evol.*, vol. 3, pp. 1–9, Nov. 2017.

[159] Y. Peng, J. Su, X. Shi, and B. Zhao, "Evaluating deep learning based network intrusion detection system in adversarial environment," in *Proc. IEEE 9th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jul. 2019, pp. 61–66.

[160] O. Faker and E. Dogdu, "Intrusion detection using big data and deep learning techniques," in *Proc. ACM Southeast Conf. (ZZZ-ACM SE)*, 2019, pp. 86–93.

[161] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "A novel two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[162] W. Tao, W. Zhang, C. Hu, and C. Hu, "A network intrusion detection model based on convolutional neural network," in *Proc. Int. Conf. Secur. Intell. Comput. Big-Data Services*, 2018, pp. 771–783.

[163] K. Kanagaraj, S. Swamynathan, and A. Karthikeyan, "Cloud enabled intrusion detector and alerter using improved deep learning technique," in *Proc. Int. Conf. Intell. Inf. Technol.*, 2018, pp. 17–29.

[164] S. Potluri, S. Ahmed, and C. Diedrich, "Convolutional neural networks for multi-class intrusion detection system," in *Proc. Int. Conf. Mining Intell. Knowl. Explor.*, 2018, pp. 225–238.

[165] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "*Deep−Full−Range*: A deep learning based network encrypted traffic classification and intrusion detection framework," *IEEE Access*, vol. 7, pp. 45182–45190, 2019.

[166] W.-H. Lin, H.-C. Lin, P. Wang, B.-H. Wu, and J.-Y. Tsai, "Using convolutional neural networks to network intrusion detection for cyber threats," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 1107–1110.

[167] C.-M. Hsu, H.-Y. Hsieh, S. W. Prakosa, M. Z. Azhari, and J.-S. Leu, "Using long-short-term memory based convolutional neural networks for network intrusion detection," in *Proc. Int. Wireless Internet Conf.*, 2018, pp. 86–94.

[168] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," *Inf. Sci.*, vol. 513, pp. 386–396, Mar. 2020.

[169] P. V. Huong, L. D. Thuan, L. T. H. Van, and D. V. Hung, "Intrusion detection in IoT systems based on deep learning using convolutional neural network," in *Proc. 6th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2019, pp. 448–453.

[170] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time web intrusion detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020.

[171] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," *Soft Comput.*, vol. 24, pp. 1–14, Nov. 2020.

[172] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Future Gener. Comput. Syst.*, vol. 113, pp. 418–427, Dec. 2020.

[173] G. Andresini, A. Appice, and D. Malerba, "Nearest cluster-based intrusion detection through convolutional neural networks," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106798.

[174] C.-M. Hsu, M. Z. Azhari, H.-Y. Hsieh, S. W. Prakosa, and J.-S. Leu, "Robust network intrusion detection scheme using long-short term memory based convolutional neural networks," *Mobile Netw. Appl.*, pp. 1–8, Jul. 2020.

[175] L. Mohammadpour, T. Ling, C. Liew, and A. Aryanfar, "A mean convolutional layer for intrusion detection system," *Secur. Commun. Netw.*, vol. 2020, Oct. 2020, Art. no. 8891185.

[176] G. Liu and J. Zhang, "CNID: Research of network intrusion detection based on convolutional neural network," *Discrete Dyn. Nature Soc.*, vol. 2020, pp. 1–11, May 2020.

[177] S. Li, "Network intrusion detection model based on improved convolutional neural network," in *Proc. Int. Conf. Cyber Secur. Intell. Anal.*, 2020, pp. 18–24.

[178] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, Mar. 2020, Art. no. 107450.

[179] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 218–224.

[180] W. Jo, S. Kim, C. Lee, and T. Shon, "Packet preprocessing in CNN-based network intrusion detection system," *Electronics*, vol. 9, no. 7, p. 1151, Jul. 2020.

[181] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.

[182] L. Zhang, J. Huang, Y. Zhang, and G. Zhang, "Intrusion detection model of CNN-BiLSTM algorithm based on mean control," in *Proc. IEEE 11th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Oct. 2020, pp. 22–27.

[183] L. Yu, J. Dong, L. Chen, M. Li, B. Xu, Z. Li, L. Qiao, L. Liu, B. Zhao, and C. Zhang, "PBCNN: Packet bytes-based convolutional neural network for network intrusion detection," *Comput. Netw.*, vol. 194, Jul. 2021, Art. no. 108117.

[184] R. V. Mendonca, A. A. M. Teodoro, R. L. Rosa, M. Saadi, D. C. Melgarejo, P. H. J. Nardelli, and D. Z. Rodriguez, "Intrusion detection system based on fast hierarchical deep convolutional neural network," *IEEE Access*, vol. 9, pp. 61024–61034, 2021.

[185] X. Kan, Y. Fan, Z. Fang, L. Cao, N. N. Xiong, D. Yang, and X. Li, "A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network," *Inf. Sci.*, vol. 568, pp. 147–162, Aug. 2021.

[186] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks," *Veh. Commun.*, vol. 29, Jun. 2021, Art. no. 100338.

[187] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 14–25, 2021.

[188] S. Zheng, "Network intrusion detection model based on convolutional neural network," in *Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Mar. 2021, pp. 634–637.

[189] S. Mishra, R. Dwivedula, V. Kshirsagar, and C. Hota, "Robust detection of network intrusion using tree-based convolutional neural networks," in *Proc. 8th ACM IKDD CODS, 26th COMAD*, Jan. 2021, pp. 233–237.

[190] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019.

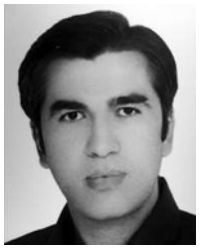
[191] S. Z. Lin, Y. Shi, and Z. Xue, "Character-level intrusion detection based on convolutional neural networks," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–8.

[192] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Jul. 2017, pp. 43–48.

[193] J. Saxe and K. Berlin, "eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys," 2017, *arXiv:1702.08568*. [Online]. Available: http://arxiv.org/abs/1702.08568
[194] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2017, pp. 712–717.
[195] M. M. U. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2017, pp. 456–462.
[196] H. Yang, L. Cheng, and M. C. Chuah, "Deep-learning-based network intrusion detection for SCADA systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–7.
[197] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A deep learning based intrusion detection method in VANET," in *Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2019, pp. 288–293.
[198] J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, and T. Kroecker, "Intrusion detection for IoT devices based on RF fingerprinting using deep learning," in *Proc. 4th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Jun. 2019, pp. 98–104.
[199] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2019, Art. no. 100198.
[200] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.
[201] S.-J. Bu and S.-B. Cho, "A hybrid system of deep learning and learning classifier system for database intrusion detection," in *Proc. Int. Conf. Hybrid Artif. Intell. Syst.*, 2017, pp. 615–625.
[202] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.
[203] S. Saraeian and M. M. Golchi, "Application of deep learning technique in an intrusion detection system," *Int. J. Comput. Intell. Appl.*, vol. 19, no. 2, Jun. 2020, Art. no. 2050016.
[204] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," *Soft Comput.*, vol. 24, no. 22, pp. 17265–17278, Nov. 2020.
[205] K. Wu, Z. Chen, and W. Li, "A novel intrusion detection model for a massive network using convolutional neural networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018.
[206] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6187–6196, Apr. 2021.
[207] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational AutoEncoder and deep neural network," *Sensors*, vol. 19, no. 11, p. 2528, Jun. 2019.
[208] K. Hara and K. Shiomoto, "Intrusion detection system using semi-supervised learning with adversarial auto-encoder," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2020, pp. 1–8.
[209] C. Zhang, X. Costa-Perez, and P. Patras, "Tiki-taka: Attacking and defending deep learning-based intrusion detection systems," in *Proc. ACM SIGSAC Conf. Cloud Comput. Secur. Workshop*, Nov. 2020, pp. 27–39.

JAN LANSKY received the M.S. degree and the Ph.D. degree in computer science (software systems) from Charles University, Prague, Czech Republic, in 2005 and 2009, respectively. He has been a Professor with the Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, since March 2009, where he has also been the Head of the Department, since September 2014. His research interests include cryptocurrencies, text compression, and databases.

SAQIB ALI received the M.Sc. degree in information systems and the Ph.D. degree in computer science from La Trobe University, Australia. He is currently an Associate Professor with the Department of Information Systems, Sultan Qaboos University, Muscat, Oman. His research interests include industrial informatics, cyber security for cyber physical systems, and business processes and automation.



MOKHTAR MOHAMMADI received the B.S. degree in computer engineering from Shahed University, Tehran, Iran, in 2003, the M.S. degree in computer engineering from Shahid Beheshti University, Tehran, in 2012, and the Ph.D. degree in computer engineering from the Shahrood University of Technology, Shahrood, Iran, in 2018. He is currently with the Department of Information Technology, Lebanese French University, Erbil, Iraq. His current research interests include signal processing, time-frequency analysis, and machine learning.

MOHAMMED KAMAL MAJEED received the B.Sc. degree in computer engineering from Tishk International University, Iraq, in 2013, and the M.Sc. degree in computer engineering from Near East University, Cyprus, in 2018. He works as assistant lecturer at Tishk International University. His current research interests include pattern recognition, machine learning, and cyber security.

SARKHEL H. TAHER KARIM received the B.Sc. degree in computer science from the University of Sulaimani, Sulaymaniyah, Iraq, in 2007 (third out of 20 graduated), and the master's degree in computer science from the Faculty of Management and Information Technology, Jamia Hamdard University, New Delhi, India, in 2011. From 2007 to 2009, he started working at the University of Sulaimani, where he was a Lecturer with the Department of Computer, College of Science, from 2011 to 2016. He has been the Head of the Computer Department, College of Science, University of Halabja, Halabja, Iraq, since 2016. His current research interests include recommender systems, social network analysis, speech, dialogue, and natural language processing, neural networks, deep learning, and the Internet of Things.

SHIMA RASHIDI was born in Iran, in 1989. She received the B.E. and M.E. degrees in computer science from the University of Tabriz, Tabriz, Iran, in 2011 and 2013, respectively. She is currently pursuing the Ph.D. degree with the University of Science and Technology, Tehran, Iran.

She is also an Assistant Lecturer with the University of Human Development, Sulaymaniyah, Iraq. Her main research interests include text mining, semi supervised learning, and social network analysis.

MEHDI HOSSEINZADEH received the B.S. degree in computer hardware engineering from Islamic Azad University, Dezfol Branch, Iran, in 2003, and the M.Sc. and Ph.D. degrees in computer system architecture from Islamic Azad University, Science and Research Branch, Tehran, Iran, in 2005 and 2008, respectively. He has authored/coauthored more than 150 publications in technical journals and conferences. His research interests include SDN, information technology, data mining, big data analytics, e-commerce, e-marketing, and social networks.

AMIR MASOUD RAHMANI received the B.S. degree in computer engineering from the Amirkabir University of Technology, Tehran, in 1996, the M.S. degree in computer engineering from the Sharif University of Technology, Tehran, in 1998, and the Ph.D. degree in computer engineering from IAU University, Tehran, in 2005. He is currently a Professor of computer engineering with the National Yunlin University of Science and Technology. He has authored/coauthored more than 350 publications in technical journals and conferences. His research interests include distributed systems, the Internet of Things, and evolutionary computing.