Extensive Analysis of Intrusion Detection System Using Deep Learning Techniques

Nishit Bhaskar Patil and Shubhalaxmi Joshi

Abstract Intrusion detection systems (IDS) is a major cyber security approach that aims to observe the status of the software and hardware components operating in a system or network. Several IDS models have been available in the literature for tackling the security issues, which can be divided into two types, namely, signature-based IDS (SIDS) and anomaly-based IDS (AIDS). Regardless of recent developments, the present IDSs still needed to enhance the detection performance, minimize the false alarms, and recognizing unknown attack. For resolving these issues, several research works have dedicated on the design of IDS via machine learning (ML) and deep learning (DL) models. In this aspect, this study intends to perform a complete review of recently developed DL models for IDS. Besides, a detailed review of various DL models designed to identify the intrusions in the network take place. In addition, an extensive analysis of the reviewed approaches is performed in terms of different aspects such as objectives, underlying methodology, dataset used, and measures. Moreover, a brief discussion of the results obtained by the DL-based IDS models is also made. At last, the possible future developments and challenges involved in the IDS models are elaborated briefly.

Keywords Deep learning · Machine learning · Intrusion detection system · Cybersecurity · Attack detection · Data classification

1 Introduction

The transformation of malicious software shows crucial challenges to the development of intrusion detection system (IDS). The malicious attack has become increasingly complex and the primary problem is to find obfuscated and unknown malware

N. B. Patil (✉)
School of Computer Science, MIT-WPU, Pune, Maharashtra, India
e-mail: nsht.patil@gmail.com

S. Joshi
Department of Master of Computer Application, Faculty of Science, MIT-WPU, Pune, Maharashtra, India

A. J. Kulkarni et al. (eds.), *Intelligent Systems and Applications*, Lecture Notes in Electrical Engineering 959, https://doi.org/10.1007/978-981-19-6581-4_16

[1]. Additionally, there has been increasing threats to security like zero-day attack developed to end internet user [2]. Thus, computer security is becoming very important as the usage of information technology has been an essential part of their day-to-day life. Intrusion is an act operated illegally or legally in transmission networks and systems that display variation from regular actions of that network. IDS is a well-equipped software or hardware-based system used to trap the intrusion at an early stage [3]. It is an integration of methods, tools, and resources that assist in identifying the intrusion and dissolving them at the right time. First line of defense, the prevention technique for intrusions like access control, authenticity, cryptography, and secure routing [4, 5]. Figure 1 illustrates the general process involved in IDS.

Initially, IDS was presented in 1980. Since then, many advanced IDS products have emerged. But still, several IDS suffer from a higher false alarm rate, generate several alerts for lower non-threatening situations that can cause severe harmful attacks to be ignored and increase the burden for security analysts [6]. Therefore, several authors aimed at designing IDS with reduced false alarm rates and high detection rates. Other challenges with current IDS are that they cannot identify unknown attacks. Since network environment changes rapidly, attack variants and novel attacks emerge continuously. Therefore, it is essential to design IDS that could identify unknown attacks. To resolve these above-mentioned issues, authors have focused on building IDS using machine learning (ML) techniques. The ML method is a type of artificial intelligence (AI) approach that could automatically determine valuable data from large data sets [7].

The ML-based IDS could attain a reasonable detection level once satisfactory training data is available, and ML model has adequate generalizability to identify novel attacks and attack variants [8]. Additionally, ML-based IDS don't depend largely on domain knowledge; hence, they are easier to construct and design. Deep learning (DL) is a subdivision of ML method which could attain remarkable performance. In comparison with conventional ML methods, DL approaches are good at handling big data [9]. Furthermore, DL techniques could automatically learn feature representation from raw information and then output results; they are practical and function in an end-to-end method. One prominent characteristic of DL is the deeper network which has numerous hidden layers. At the same time, conventional ML techniques [10], like *k*-nearest neighbors (*K*NN) and support vector machines (SVM), contains none or only one hidden layer. Hence, this conventional ML method is known as shallow model.

This study concentrates on the survey of recently presented DL models for IDS. This study examines the existing 35 DL based intrusion detection approaches based on the performance evaluation, determines the research gap, and highlights the reviewed works. All the articles selected for analysis are based on the performance outcome and its accuracy results. The reviewed methods are examined in different ways such as objectives, methodology used, datasets used, and performance measures. In addition, an expressive and comparison study of the surveyed DL enabled IDS models takes place by offering a tabular format. Then, the performance analysis of the different DL models takes place and identifies the optimal solutions. Lastly, the research issues and potential future scope of the research are highlighted

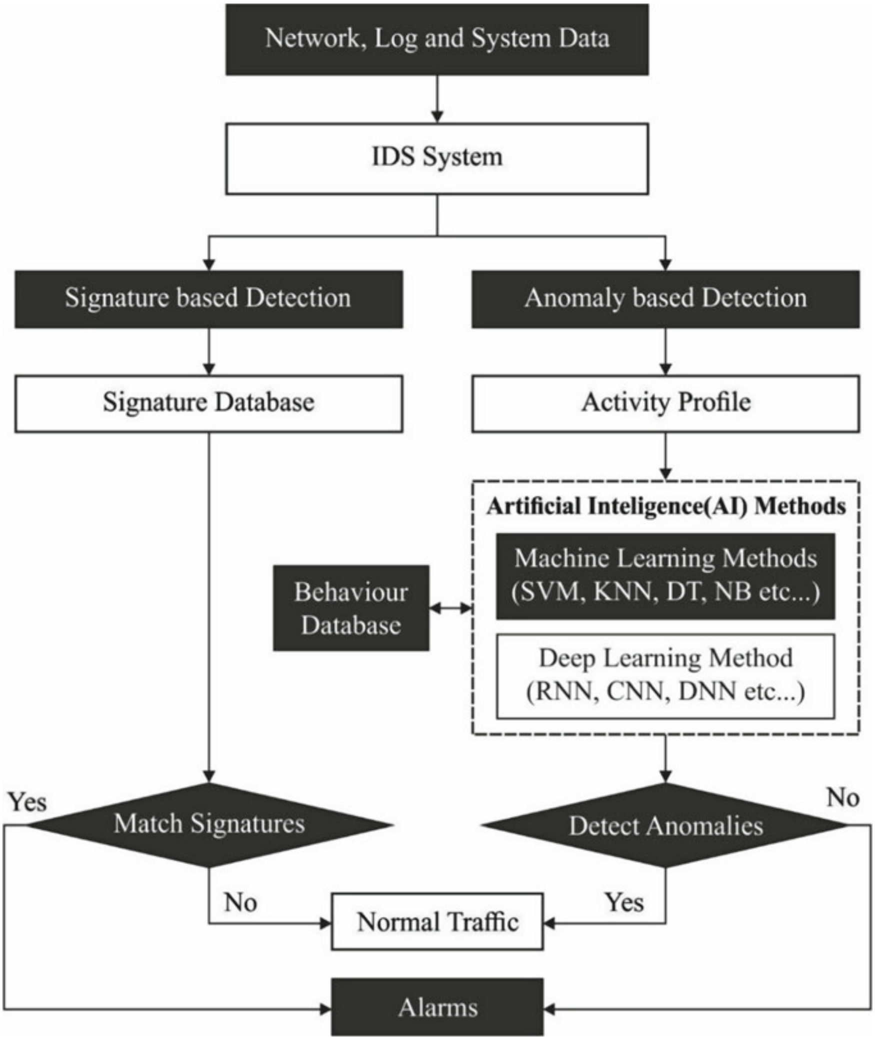
Network, Log and System Data
IDS System
Signature based Detection
Anomaly based Detection
Signature Database
Activity Profile
Artificial Inteligence(AI) Methods
Machine Learning Methods (SVM, KNN, DT, NB etc...)
Deep Learning Method (RNN, CNN, DNN etc...)
Behaviour Database
Yes
Match Signatures
No
Detect Anomalies
No
Yes
Normal Traffic
Alarms

Fig. 1 .

with objectives such as evaluating an effective intrusion detection system model from the different datasets and assessing machine learning based optimization model that will be applied to detect and classify intrusions along with its performance evaluation on parameters such as Precision, Recall, *F*-Score, and Computational Time and Accuracy.

2 Review of Deep Learning Based IDS Models

In these subsection, a detailed review of various DL-based solutions developed for IDS is shown in Table 1. Farahnakian et al. [11] introduced a DL technique to IDS. This technique utilizes Deep Autoencoder (DAE) as most famous DL technique. The presented DAE technique was trained from a greedy layer-wise fashion for avoiding over-fit and local optimum. Hanselmann et al. [12] regarded a novel unsupervised learning approach called CANet. Familiar to us, an initial DL based IDS that manages the data structure of maximum dimension CAN bus, in which varying message kinds are sent at varying times. This technique was estimated on real and synthetic CAN data. An evaluation with preceding ML techniques demonstrates that CANet exhibits them by an important margin.

In Boukhalfa et al. [13], a novel idea to Network IDS (NIDS)-based LSTM for recognizing menaces and for obtaining long-term memory on them, for stopping a novel attack that is similar to the recent ones, and simultaneously, for containing a single mean to block intrusion. The simulated outcome is proved that novel technique LSTM is more effective, it is efficiently memorizing and differentiate among traffics: normal and attack, from both situations of classifications, binary and multi-classification. Yin et al. [14] presented a DL technique to IDS utilizing recurrent neural networks (RNN-IDS). Also, it can be analyzed the efficiency of the model from binary as well as multiclass classifications, and the amount of neurons and varying learning rate influence the efficiency of the presented technique. It can be related to individuals of J48, ANN, RF, SVM, and other ML techniques presented by the preceding researcher on the benchmark dataset.

Kunang et al. [15] introduced a DL-based IDS utilizing a pre-training approach with deep autoencoder (PTDAE) related to DNN. These techniques are established utilizing hyperparameter optimized methods. This investigation offers an alternative solutions to DL framework techniques with automatic hyperparameter optimized procedure which relates grid as well as random search approaches. The automated hyperparameter optimized technique uses defines the value of hyperparameter and an optimum categorical hyperparameter structure for improving detection efficiency. Fatani et al. [16] examined an effective AI based procedure to IDS from IoT systems. It can control the progress of DL and metaheuristics (MH) techniques which permitted its efficacy from resolving difficult engineering issues. It can be present the feature removal technique utilizing the CNNs for extracting relevant features. Besides, it can progress a novel FS technique utilizing a novel different of transient search optimization (TSO) technique is named TSODE, utilizing the operator of differential evolution (DE) technique.

In Kanna and Santhi [17], a precise IDS technique was presented by utilizing a unified method of optimized CNN (OCNN) and hierarchical multi-scale LSTM (HMLSTM). The presented IDS method carries out the pre-processed, feature removal with testing and training of network and last classification. In this method, the lion swarm optimization (LSO) was utilized for tuning the hyperparameter of CNN to an optimum configuration of learning spatial features. Aleesa et al. [18]

Table 1 Comparison of different DL-based IDS models

References	Year	Objective	Methodology used	Dataset used	Performance measures
Farahnakian et al. [11]	2018	To detect intrusions and avoid overfitting	DAE	KDD-CUP'99 dataset	Accuracy, detection rate and false alarm rate
Hanselmann et al. [12]	2020	To design unsupervised IDS for CAN	CANet	Real and synthetic CAN data	Accuracy, TPR/TNR
Boukhalfa et al. [13]	2020	To detect and block intrusions in the network	LSTM	NSL KDD	Accuracy, sensitivity, false positive rate, precision, and recall
Yin et al. [14]	2017	To design an IDS for binary and multi-class classification	RNN-IDS	NSL-KDD dataset	Accuracy, detection rate, and FPR
Kunang et al. [15]	2021	To develop IDS with hyperparameter optimization process	PTDAE-DNN	NSL-KDD, and CSE-CIC-ID2018	Precision, recall, accuracy, *F*-score, training time
Fatani et al. [16]	2021	To introduce a AI based solution for IDS	CNN + TSODE	KDDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017	Precision, recall, accuracy, *F*-score
Kanna and Santhi [17]	2021	To devise automated IDS using spatio and temporal features	OCNN + HMLSTM	NSL-KDD, ISCX-IDS, and UNSWNB15	Accuracy
Aleesa et al. [18]	2021	To improvise the UNSW-NB15 dataset for DL models	Deep-IDS	Improved UNSW-NB15 dataset	Accuracy
Lee and Park [19]	2021	To address imbalance data classification problem for IDS	GAN	CICIDS 2017 dataset	Precision, recall, accuracy, *F*-score

(continued)

Table 1 (continued)

References	Year	Objective	Methodology used	Dataset used	Performance measures
Liu et al. [20]	2021	To design a cascaded IDS with distributed *K*-means, RF, and DL models	CNN, LSTM + ADASYN	NSL-KDD and CIS-IDS2017 datasets	Accuracy, TPR, time cost
Ullah and Mahmoud [21]	2021	To devise a new DL based anomaly identification model for IoT environment	CNN	BoT-IoT, IoT network intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets	Precision, recall, accuracy, *F*-score
Aldallal and Alisa [22]	2021	To develop a hybrid IDS for cloud platform	GA + SVM	CICIDS2017 dataset	Accuracy, detection rate
Abusitta et al. [23]	2019	To present a co-operative IDS for cloud platform	DA + DNN	KDD Cup'99 dataset	Accuracy
Zhou et al. [24]	2021	To propose a GNN based IDS for IoT environment	HAA with GNN + RWR	UNSW-SOSR2019	Precision
Al Jallad et al. [25]	2019	To project a DL based IDS model for big data	LSTM	MAWI dataset	Detection rate
Mighan and Kahani [26]	2021	To develop a hybrid ML and DL model for IDS	Stacked autoencoder	UNB ISCX 2012 dataset	accuracy, *f*-measure, sensitivity, precision, and time
Vinayakumar et al. [27]	2019	To develop an intelligent IDS model using DNN	DNN	NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017	Precision, recall, accuracy, *F*-score, TPR, ROC
Kasongo and Sun [28]	2020	To design a new IDS for wireless networks	FFDNN + WFEU	UNSW-NB15	Accuracy
Shone et al. [29]	2018	To introduce a DL model for NIDS	NDAE	KDD Cup'99 and NSL-KDD dataset	Precision, recall, *F*-score, accuracy, and time

(continued)

Table 1 (continued)

References	Year	Objective	Methodology used	Dataset used	Performance measures
Kasongo and Sun [30]	2019	To present a DL model with feature selection scheme for IDS	FFDNN	NSL-KDD dataset	Accuracy, precision-recall curve
Hu et al. [31]	2021	To design sensitive IDS model	IDSDL + CSI + DNN	Own dataset	Accuracy
Mendonça et al. [32]	2021	To develop a fast DL model for IDS	Tree-CNN hierarchical model	CICIDS2017 dataset	Detection accuracy, execution time
Toldinas et al. [33]	2021	To project NIDS model using multi-stage DL	ResNet50	UNSW-NB15 and BOUN Ddos	Precision
Khan [34]	2021	To introduce a hybrid IDS model	HCRNNIDS	CSE-CIC-DS2018 dataset	Precision, recall, $F1$-score, and DR
Ashiku and Dagli [35]	2021	To present a NIDS model using DL concepts	DNN	UNSW-NB15 dataset	Accuracy, detection rate
Wani and Khaliq [36]	2021	To provide a SDN based DL model for IDS	DL classifier	IDSIoT-SDL	Sensitivity, detection rate, accuracy, FAR
Jothi and Pushpalatha [37]	2021	To develop IDS for IoT	LSTM	CIDDS-001, UNSWNB15, and KDD datasets	Accuracy, precision, and recall
Haghighat and Li [38]	2021	To project voting based DL model	VNN	KDDCUP'99 and CTU-13	Precision, recall, F-score, accuracy, FPR, and FNR
Yousefnezhad et al. [39]	2021	To design ensemble model for IDS	KNN + SVM + DL model	UNSW-NB15, CICIDS2017, and NSL-KDD	Precision, recall, accuracy, F-score
Mayuranathan et al. [40]	2021	To detect DDoS in cloud environment	RHS model + RBM	KDD'99 dataset	Sensitivity, specificity, Kappa, accuracy, F-score

enhance UNSW-NB15 data set that utilized with DL as old ML approaches are taken as much time and the size of data set is not influence the efficiency of ML approaches, but the size of utilized data set affects the efficacy of DL approaches.

Lee and Park [19] resolved data imbalance by utilizing the generative adversarial networks (GAN) technique that is an unsupervised learning approach of DL that created novel virtual data same as recent data. It is also presented a model which is classified as RF for identifying detection efficiency after addressing data imbalance dependent upon GAN. In Liu et al. [20], an ID technique that relates ML with DL was presented. This technique utilizes the *k*-means and RF techniques as classifiers, and distributed computing of these techniques are executed on Spark platform for rapidly classifying normal as well as attack events. Next, with utilizing the CNN, LSTM, and other DL techniques, the event judged as abnormal is more classified as to varying attack type lastly. Currently, adaptive synthetic sampling (ADASYN) was selected for solving the unbalanced data set.

Ullah and Mahmoud [21] develop and design an anomaly-based IDS for IoT networks. Firstly, a CNN method is applied for creating a multi-class classification method. Then, the presented method is carried out through CNN models in 1D, 2D, and 3D. The generation and processing of features focus on the actual network traffic flow. They developed four data sets using this approach and then integrate them by rising the number of attack classes. Aldallal and Alisa [22], proposed a ML-based hybrid IDS. We integrated SVM and GA methods with an advanced fitness function designed for evaluating performance of the system. This scheme was investigated by the CICIDS2017 data set that has common and normal attacks. These two GA and SVM algorithms have been implemented in parallel to attain two ideal objectives: obtain the optimal set of features with the highest performance.

Abusitta et al. [23] present a ML-based IDS that effectively employs the past feedback data to make decisions. Especially, the presented method is depending on a Denoising Autoencoder (DA), i.e., employed as a fundamental element to create a DNN system. The power of DA exists in its capacity of learning the way to recreate IDS feedback from partial feedback. It enables to periodically decide suspected intrusion without comprehensive feedback from the IDS. Zhou et al. [24], introduced a hierarchical adversarial attack (HAA) technique, targeting the graphical neural network (GNN)-related IDS in the IoT system constrained resources. A hierarchical node election method based random walk with restart (RWR) is designed for selecting a group of susceptible nodes with higher attack importance, with the consideration of the overall loss changes and structural features within the targeted IoT networks.

Al Jallad et al. [25] present a resolution to identify new threats with lower false positive and high detection rates than previously employed IDS, as well as identify contextual and collective security attacks. They attain outcomes through networking Chatbot, a Deep RNN: LSTM on topmost Apache Spark Framework which contains input of traffic aggregation and traffic flow and the outcome is a language of two words, abnormal or normal. Mighan and Kahani [26] present a hybrid system that integrates the benefits of ML and deep network systems. At first, SAE system is utilized for latent feature extraction, which follows various classification-based IDSs, like SVM, RF, DT, and NB that is utilized for efficient and fast detection of intrusion in large network traffic data.

In Vinayakumar et al. [27], a DNN system, a kind of DL method, is used to design an effective and flexible IDSs for detecting and classifying unpredictable and unforeseen cyber-attacks. The rapid changes in network behavior and continues development of attacks make it essential for evaluating different data sets that are produced by the dynamic and static models. This kind of study facilitates the finding of the optimal model that could perform efficiently in identifying upcoming cyber-attacks. Kasongo and Sun [28] present a FFDNN wireless IDSs with a wrapper based feature extraction unit (WFEU). The WFEU employs the extra trees model for creating a best possible feature vector. The efficacy and efficiency of the WFEU-FFDNN are examined according to the AWID and UNSW-NB15 IDS data sets.

Shone et al. [29] proposed a Dl method for IDS called non-symmetric deep auto-encoder (NDAE). Moreover, the authors introduced DL classification technique via stacked NDAE. The presented classification method was executed in GPU-assisted TensorFlow and estimated by the standard NSL-KDD and KDD Cup'99 data sets. Kasongo and Sun [30] designed an IDS based DL method using FFDNN together with a filter-based feature selection method. The presented method can be estimated by the popular data mining (NSL-KDD) and NSL-knowledge discovery datasets and it is compared with the current ML algorithms.

Hu et al. [31] presented an IDS-based DL (IDSDL) with fine grained channel state information (CSI) for free the AP place. In CSI stage propagation modules decomposition technique was implemented for obtaining blurred elements of CSI stage on various paths as further sensitive detection signals. In CNN of DL was utilized for enabling the computer for learning as well as detecting intrusion without removing numerical features. In Mendonça et al. [32], a novel IDS dependent upon Tree-CNN hierarchical technique with Soft-Root-Sign (SRS) activation purpose was presented. To performance assessment, this method was executed in medium-sized company, analyzing the level of difficulty of presented solutions.

Toldinas et al. [33] present a novel manner to network ID utilizing multistage DL image detection. The network feature was altered as to 4 channel (Alpha, Blue, Red, and Green) images. Images are utilized for classification for testing as well as training the pretrained DL technique ResNet50. In Khan [34], a convolutional recurrent neural network (CRNN) was utilized for creating a DL-based hybrid ID structure that forecasts and categorizes malicious cyberattacks from the networks. Ashiku and Dagli [35] presents utilize of DL structures for developing a resilient and adaptive network IDS for detecting as well as classifying network attacks. The emphasis is DL or DNNs are enable flexible IDS with learning capacity for detecting and novel or zero-day network behavioral feature, consequently emitting the system intruders and decreasing the risks of compromises. In Wani and Khaliq [36], an SDN based IDS was presented that utilizes DL classifier to detection of anomaly from IoT. The presented IDS doesn't burden the IoT device with security profile. The presented work was implemented in simulated environments. The outcomes of the experimental test are estimated utilizing different matrices and related to other relevant techniques.

In Jothi and Pushpalatha [37], a novel IDS was presented utilizing powerful DL techniques. Motivated by LSTM benefits, whale integrated LSTM (WILS) network was presented for designing intelligent IDS for detecting the range of distinct states of threat on IoT networks. The system includes four important functions: (i) Data gathering unit that profiles the regular efficiency of IoT device linked from the network, (ii) identify the malicious device on the networks if an attack was happening, (iii) forecasts the kind of attacks utilized from the network. In Haghighat and Li [38], a novel voting-based DL structure is named VNN has presented for taking the benefits of some types of DL frameworks. Regarded as many methods generated by distinct features of data and many DL frameworks, VNN offers the capability for aggregating optimum methods for creating further accurate and robust outcomes. So, VNN uses security specialists for detecting further difficult attacks.

Yousefnezhad et al. [39] implement ensemble methods for enhancing the efficiency of ID and simultaneously, reduce the FAR. It can be utilized *k*NN tor multiclass classifier as well as SVM for approaching the classification issue from normally based detections. For combining several outcomes, it can be the Dempster–Shafer approach in that there are possibilities of explicit retrieval of uncertainty. In addition, it can be employed DL to remove features for training the instances, chosen by the instance selective technique dependent upon ensemble margin. Mayuranathan et al. [40] present an effective feature subset selection-based classification method to detect DDoS attacks. For detecting the DDoS attacks from IDS, an optimum feature set was chosen with maximal detection by utilizing of random harmony search (RHS) optimized method. If the features were chosen, a DL-based classifier method utilizing RBM was executed for detecting the DDoS.

3 Performance Analysis

This section inspects the recently developed DL models for IDS available in the literature. Table 2 offers the comparative analysis of the DL models interms of different measures. Figure 2 investigates the prec_n, reca_l, and F_{score} analysis of the DL models. The figure reported that the DNN model has obtained lower prec_n, reca_l, and F_{score} values of 0.81, 0.785, and 0.765, respectively. At the same time, the CCNN model has obtained slightly enhanced prec_n, reca_l, and F_{score} of 0.815, 0.791, and 0.76. Moreover, the conditional VAE, FNN, and MLESM-RNN techniques have resulted in moderate prec_n, reca_l, and F_{score} values. Furthermore, the RNN model has tried to accomplish merate prec_n, reca_l, and F_{score} of 0.831, 0.833, and 0.82, respectively. However, the DAE-DNN model has resulted in higher prec_n, reca_l, and F_{score} of 0.86, 0.833, and 0.82, respectively.

The accu_y analysis of the DL models is carried out in Fig. 3. The figure reported that the CCNN and DNN models have gained lower accu_y values of 0.791 and 0.785. In line with, the FNN, conditional VAE, RNN, and MLESM-RNN techniques have obtained moderate accu_y values of 0.803, 0.801, 0.813, and 0.804, respectively. But, the DAE-DNN technique has resulted in a maximum accu_y of 0.833.

Table 2 Comparative analysis of DL technique for IDS interms of different measures

Methods	Precision	Recall	Accuracy	$F1$-score
CCNN	0.815	0.791	0.791	0.76
FNN	0.821	0.803	0.803	0.815
RNN	0.831	0.813	0.813	0.793
Conditional VAE	0.816	0.801	0.801	0.791
Deep neural network	0.81	0.785	0.785	0.765
MLESM-RNN	0.819	0.804	0.804	0.792
DAE-DNN	0.86	0.833	0.833	0.82

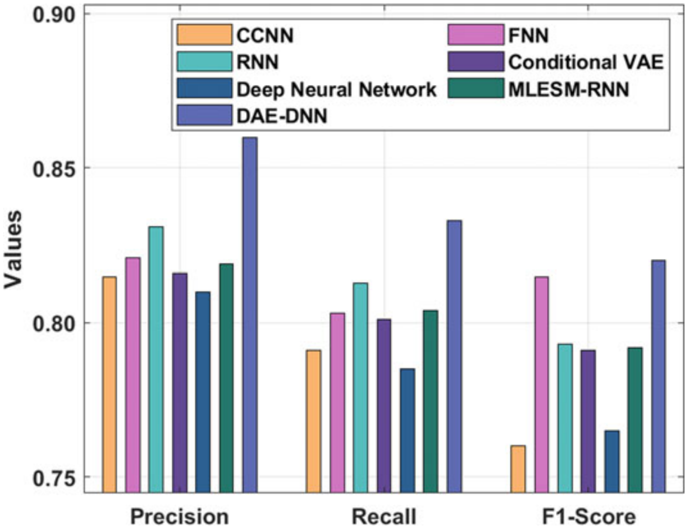

Fig. 2 Comparative analysis of DL techniques with varying measures

4 Challenges and Future Developments

The usage of an appropriate data set is one of the major problems in the development of deep learning-based IDS. The presented method doesn't offer reliable performance result, because they are based on the NSL- or KDD KDD99 benchmark data sets, that has older traffic, don't have real-time properties, and don't characterize current traffic behaviors and attack scenarios. Hence, attaining traffic from simulated environment could overcome this problem by investigating current data sets, like the N-BaIoT IoT [41], and CICIDS2017 IDS intrusion prevention system (IPS) datasets [42]. Also, the published dataset is available for several fields, like industrial control systems (ICS). As well, the comparison between distinct DL approaches that are carried out in isolation doesn't offer a reasonable comparison based on efficiency and effectiveness. This is because of differences in: (1) preprocessing (2) deep

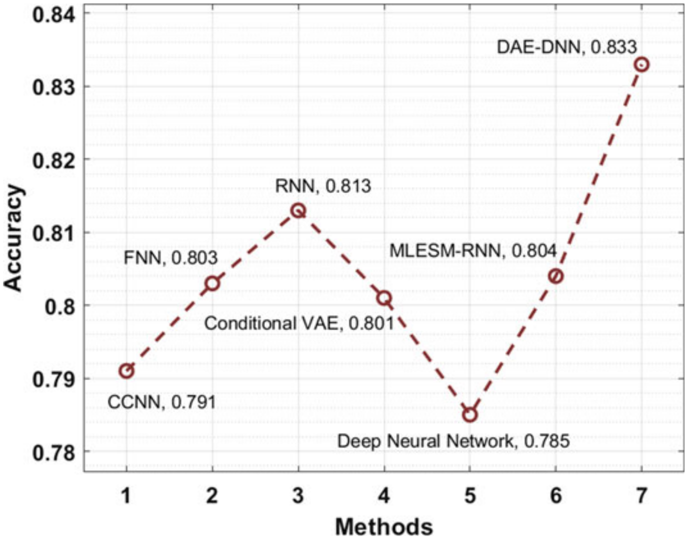

Fig. 3 Accuracy analysis of DL technique

network configuration, (3) hardware platforms (4) the used dataset, and (5) part of the data set, viz., adapted. Hence, it is necessary for further comparative analysis that uses common affecting factors and unified computing platforms for distinct DL frameworks to attain a reasonable result.

Yet, the DL methods does not cover intrusion detection in different fields. Thus, it is essential to reconsider the IDS problems in several fields like smart grids, 5G, several IoT platforms, and SCADA that have been previously analyzed by shallow ML and other anomaly detection methods. Extensibility to distinct fields requires a data set that truly reflects the targeted environments and attains remarkable outcomes. Several DL-based IDS based on GPUs and CPUs for intense off-line trained computation. In response to tremendous growth, chip vendor has created innovative AI accelerator; the AI chip markets are predicted to attain $66.3 billion in 2025 [43]. The more commonly used chips are application-specific integrated circuit (ASIC), the field programmable gate array (FPGA), and the neural network processing unit (NNPU), along with the Edge TPU, a tiny AI accelerator published in 2018 by Google for IoT device. Today's IoT devices and smartphones are armed with these innovative chips. Thus, leveraging this development to perform study will generate real-time prototype, instead of trusting offline data sets. Additionally, it will permit the advancement of innovative IDS for the restricted devices. Additional research of hybrid DL frameworks like GAN model is essential. It is valuable for leveraging DL method to change from collaborative IDS to collaborative DL-based IDS.

5 Conclusion

With the emergence of advanced technologies and the drastic increase in data generation, several research communities have investigated the design of DL models to detect intrusions. This survey extensively analyses and investigates the different DL based IDS models available in the literature. The reviewed methods are examined in different ways such as objectives, methodology used, datasets used, and performance measures. In addition, a comparative and descriptive analysis of the surveyed DL-based IDS models takes place by offering a side-by-side comparison in a tabular form. Then, the performance analysis of the different DL models takes place and identifies the optimal solutions. Lastly, the open research issues and future scope of the research are highlighted.

References

1. Sadreazami H, Mohammadi A, Asif A, Plataniotis KN (2018) Distributed-graphbased statistical approach for intrusion detection in cyber-physical systems. IEEE Trans Sig Inf Process Netw 4(1):137–147
2. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336
3. Shafi K, Abbass HA (2013) Evaluation of an adaptive genetic-based signature extraction system for network intrusion detection. Pattern Anal Appl 16(4):549–566
4. Pasqualetti F, Dörfler F, Bullo F (2013) Attack detection and identification in cyber-physical systems. IEEE Trans Autom Control 58(11):2715–2729
5. Meshram A, Haas C (2017) Anomaly detection in industrial networks using machine learning: a roadmap. In: Beyerer J, Niggemann O, Kühnert C (eds) Machine learning for cyber physical systems: selected papers from the international conference ML4CPS 2016. Springer, Berlin, pp 65–72
6. Hoque MAM, Bikas MAN (2012) An implementation of intrusion detection system using genetic algorithm. Int J Netw Secur Appl 4:2
7. Creech G, Hu J (2014) A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns. IEEE Trans Comput 63(4):807–819
8. Alazab A, Hobbs M, Abawajy J, Khraisat A, Alazab M (2014) Using response action with intelligent intrusion detection and prevention system against web application malware. Inf Manag Comput Secur 22(5):431–449
9. Chebrolu S, Abraham A, Thomas JP (2005) Feature deduction and ensemble design of intrusion detection systems. Comput Secur 24(4):295–307
10. Koc L, Mazzuchi TA, Sarkani S (2012) A network intrusion detection system based on a hidden Naïve Bayes multiclass classifier. Exp Syst Appl 39(18):13492–13500
11. Farahnakian F, Heikkonen J (2018) A deep auto-encoder based approach for intrusion detection system. In: 2018 20th international conference on advanced communication technology (ICACT). IEEE, pp 178–183
12. Hanselmann M, Strauss T, Dormann K, Ulmer H (2020) CANet: an unsupervised intrusion detection system for high dimensional CAN bus data. IEEE Access 8:58194–58205
13. Boukhalfa A, Abdellaoui A, Hmina N, Chaoui H (2020) LSTM deep learning method for network intrusion detection system. Int J Electr Comput Eng 10(3):2088–8708
14. Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5:21954–21961

15. Kunang YN, Nurmaini S, Stiawan D, Suprapto BY (2021) Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. J Inf Secur Appl 58:102804
16. Fatani A, Abd Elaziz M, Dahou A, Al-Qaness MA, Lu S (2021) IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access 9:123448–123464
17. Kanna PR, Santhi P (2021) Unified deep learning approach for efficient intrusion detection system using integrated spatial-temporal features. Knowl Based Syst 226:107132
18. Aleesa A, Younis MOHAMMED, Mohammed AA, Sahar N (2021) Deep-intrusion detection system with enhanced unsw-Nb15 dataset based on deep learning techniques. J Eng Sci Technol 16(1):711–727
19. Lee J, Park K (2021) GAN-based imbalanced data intrusion detection system. Pers Ubiquit Comput 25(1):121–128
20. Liu C, Gu Z, Wang J (2021) A hybrid intrusion detection system based on scalable *K*-means+ random forest and deep learning. IEEE Access 9:75729–75740
21. Ullah I, Mahmoud QH (2021) Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access 9:103906–103926
22. Aldallal A, Alisa F (2021) Effective intrusion detection system to secure data in cloud using machine learning. Symmetry 13(12):2306
23. Abusitta A, Bellaiche M, Dagenais M, Halabi T (2019) A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Futur Gener Comput Syst 98:308–318
24. Zhou X, Liang W, Li W, Yan K, Shimizu S, Kevin I, Wang K (2021) Hierarchical adversarial attacks against graph neural network based IoT network intrusion detection system. IEEE Int Things J
25. Al Jallad K, Aljnidi M, Desouki MS (2019) Big data analysis and distributed deep learning for next-generation intrusion detection system optimization. J Big Data 6(1):1–18
26. Mighan SN, Kahani M (2021) A novel scalable intrusion detection system based on deep learning. Int J Inf Secur 20(3):387–403
27. Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7:41525–41550
28. Kasongo SM, Sun Y (2020) A deep learning method with wrapper-based feature extraction for wireless intrusion detection system. Comput Secur 92:101752
29. Shone N, Ngoc TN, Phai VD, Shi Q (2018) A deep learning approach to network intrusion detection. IEEE Trans Emerg Top Comput Intell 2(1):41–50
30. Kasongo SM, Sun Y (2019) A deep learning method with filter-based feature engineering for wireless intrusion detection system. IEEE Access 7:38597–38607
31. Hu Y, Bai F, Yang X, Liu Y (2021) IDSDL: a sensitive intrusion detection system based on deep learning. EURASIP J Wirel Commun Netw 2021(1):1–20
32. Mendonça RV, Teodoro AA, Rosa RL, Saadi M, Melgarejo DC, Nardelli PH, Rodríguez DZ (2021) Intrusion detection system based on fast hierarchical deep convolutional neural network. IEEE Access 9:61024–61034
33. Toldinas J, Venčkauskas A, Damaševičius R, Grigaliūnas Š, Morkevičius N, Baranauskas E (2021) A novel approach for network intrusion detection using multistage deep learning image recognition. Electronics 10(15):1854
34. Khan MA (2021) HCRNNIDS: hybrid convolutional recurrent neural network-based network intrusion detection system. Processes 9(5):834
35. Ashiku L, Dagli C (2021) Network intrusion detection system using deep learning. Proc Comput Sci 185:239–247
36. Kavitha T, Mathai PP, Karthikeyan C et al (2021) Deep learning based capsule neural network model for breast cancer diagnosis using mammogram images. Interdiscip Sci Comput Life Sci. https://doi.org/10.1007/s12539-021-00467-y
37. Cyril CPD, Beulah JR, Subramani N, Mohan P, Harshavardhan A, Sivabalaselvamani D (2021) An automated learning model for sentiment analysis and data classification of Twitter data using balanced CA-SVM. Concurr Eng Res Appl 29(4):386–395

38. Reshma G, Al-Atroshi C, Nassa VK, Geetha B et al (2022) Deep learning-based skin lesion diagnosis model using dermoscopic images. Intell Autom Soft Comput 31(1):621–634
39. Bhukya RR, Hardas BM, Anil Kumar TC et al (2022) An automated word embedding with parameter tuned model for web crawling. Intell Autom Soft Comput 32(3):1617–1632
40. Wani A, Khaliq R (2021) SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). CAAI Trans Intel Tech
41. Berlin MA, Tripathi S et al (2021) IoT-based traffic prediction and traffic signal control system for smart city. Soft Comput. https://doi.org/10.1007/s00500-021-05896-x
42. Haghighat MH, Li J (2021) Intrusion detection system using voting-based neural network. Tsinghua Sci Technol 26(4):484–495
43. Yousefnezhad M, Hamidzadeh J, Aliannejadi M (2021) Ensemble classification for intrusion detection via feature extraction based on deep Learning. Soft Comput 25(20):12667–12683