Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 2990- 3000
Research Article

Deep Learning Algorithms for Intrusion Detection Systems: Extensive Comparison Analysis

Ch Sekhar[a], K Venkata Rao[b], MHM Krishna Prasad[c]

[a]Research Scholar, Dept of Computer Science and Engineering, JNTU Kakinada
[b] Professor, Dept of Computer Science and Engineering, Vignan's IIT, Visakhapatnam
[c]Professor, Dept of Computer Science and Engineering, JNTU Kakinada
[a]sekhar1203@gmail.com, [b] vrkoduganti@gmail.com,[c]krishnaprasad.mhm@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: The network of systems is facing threats from the various attacks, for that a software application needed to regular monitoring the network. Intrusion Detection System (IDS) is application software that monitors the traffic of the network for any unusual activity and raises the alarms when such activity found. The existing IDSs still face troubles in improving the identification accuracy, warning rate not overcoming and identifying mysterious assaults. To take care of the above issues, numerous researcher works going by the researchers have concentrated on creating IDSs that exploit. This survey presents modern approaches in Intrusion Detection System (IDS) applying deep learning models, which have attained great fortune newly, especially in the domain of computer vision, natural language processing, and image processing. In this study, a thorough survey of deep learning methods used by various researches on IDS. This study also proposes a comparison among various deep learning algorithms implemented on KDD Cup, NSL-KDD and UNSW-NS15 data sets.

Keywords: NIDS, HIDS, IDS, Deep Learning

1. Introduction

Today, the quantity of Internet clients is ceaselessly expanding, alongside new system administrations. As the web develops, network security issues have gotten progressively genuine. Numerous security vulnerabilities are uncovered and abused by assaults. Intrusion Detection System (IDS) is application software that monitors the traffic of the network for any unusual activity and raises the alarms when such activity found. However, Network intrusion detection system performance is generally low accurate when it is subjected to new and unfamiliar attacks. The solution for the same can be processed by recording the datasets and almost half of the anonymous attacks on the testing dataset never appear in the training dataset, and it is challenging for all classifiers to detect attacks. The detection of any unknown attack and unknown data type. One of the essential concerns to consider is to make sure the data is clean. On the other hand, prior to the known attacks, we can also detect unknown attacks.

Networks are increasingly influencing modern life, making information security a significant research area. Cybersecurity strategies include, in particular, intrusion detection systems, firewalls, antivirus software. From the internal and external threats, those techniques protect from the networks, and an ID is a form of a monitoring device that plays an important role in helping to protect network security by tracking the software and hardware system that is operating in a network. Several mature IDS products have emerged since then. Nevertheless, most IDSs also Suffer massive false warning levels, producing frequent warnings for low non-threatening circumstances, which enhances the pressure on security analysts and may cause harmful attacks to be missed. Several researchers have thus concentrated on improving IDSs with high recognition levels and reducing false warning rates. A potential issue with current IDSs is the failure to track unexplained assaults. When network dynamics are evolving rapidly, types of attacks and new attacks are continuously emerging. Therefore, the development of IDSs that can identify unknown threats is essential.

The figure 1 below shows, the role of IDS, its place behind the firewall scanning for patterns in network traffic that might intimate malicious activity. Thus, IDSs are used as the next and the final level of defence in any protected network against attacks that breach other defences.

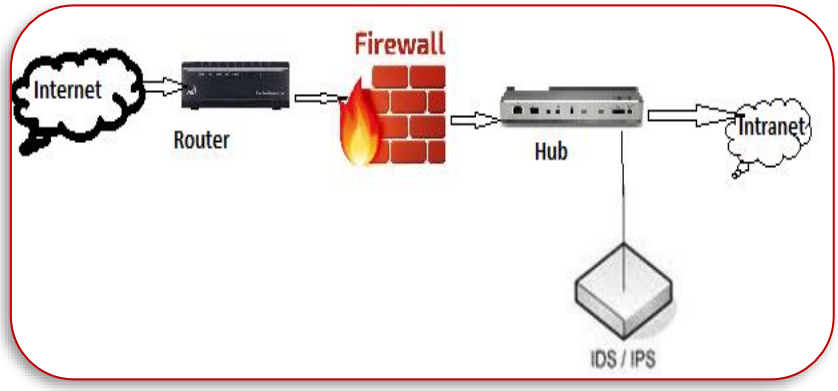


Figure1: Intrusion Detection System

To identify the unseen security attacks, computer network needs a reliable monitoring system from time to time. In 1980, the network monitoring system came named as the Intrusion detection system. It suffers from the high false alarm rate, and it leads to unable to find the sever security attacks. Numerous researchers have converged on improving IDSs with higher detection rates and reduced false alarm rates[1,2]. An Intrusion Detection System (IDS), a considerable investigation accomplishment in the data security field, can recognise an attack, which could be a progressing intervention or an intrusion that has just happened. An IDS based on the behaviour of the network, security issues categorised as four classes of attacks with the label. The attack types are User to Root, Probing, Root to Local, and Denial of Service.

Machine learning procedures have been widely used in intrusion detection for several years. Nevertheless, these procedures still suffer from the shortage of labelled dataset, huge expenses and low efficiency. To enhance the accuracy of the classification and minimise the training time, this survey suggests an efficient deep learning approach used by various researches for IDS[13,2]. In this study, comparative among the dataset, methods of reduction of dimensionality, attack identification methods, various classification techniques, testing methods, suitable evaluation metrics. The review concludes by deriving various hurdles and insights for future research directions[5].

The aim of this study is as follows: Section 2 describes brief about various types of attacks, Intrusion Detections Systems and performance metrics for IDS. In section 3 describing the datasets available to use for IDS. In part 4, highlighted that deep learning models suitable for IDS performance by various researchers. In part 5, It summarily examines 20 articles which are using machine learning and deep learning techniques for their IDSs.

2. Review On IDS

2.1 Intrusion Types:

A network of systems, an attack is caused in any manner to alter the original information. An unknown person was trying to retrieve the data from the computer network systems illegally. An attack trying to change the processing operation, destroy the data, theft the data. The various attacks based on their nature shown in figure 2 below. Majorly attacks classified as based on the source of the attack and its behaviour[6].

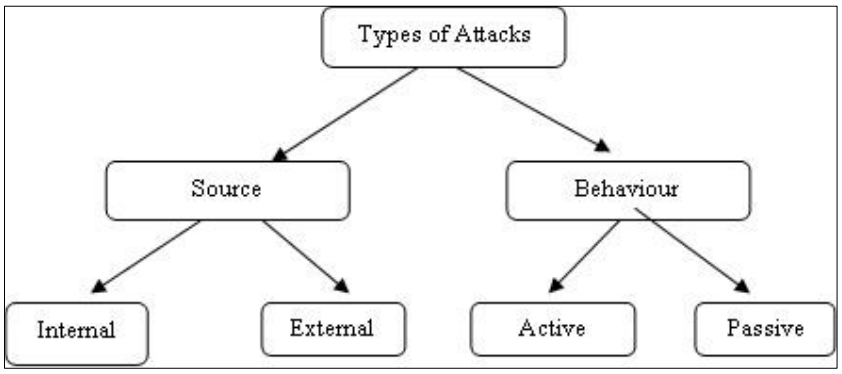


Figure 2: Types of Attacks

The source of an attack can be of either from Internal or external sources. Internal source attacks, the internal person who wants to get access to the network, and do the various malicious activities to gain access as a new

node. The external source, attacks occurred due to the outside of the network node trying to access the network. External persons or attackers are targeting the network in terms of congestion, wrong routing.

Behavioural-based attacks are of two types, active and passive attacks. Active attacks are which an intruder initiates calls to disrupt the network's regular operation, and Passive attacks are network intruder intercepts data travelling through the network [8].

Table 1: Behavioural-based attack/Intrusions [6, 8]

Attack type	Name of Attack	Description
Active	Spoof	While an attacker imitates someone else's machine so that it will produce assaults against network hosts, get pass entry to control, steal facts, or unfold malware.
	Black Hole	It is a packet drop attack in network traffic.
	Gray Hole	Acts like a malicious node to drop malicious packets, however later switches again to every day.
	Malicious Packet Dropping	If the router of malicious trying to drop all packets which are entered, and of type DDoS.
Passive Attacks	Eavesdropping	Network layer assaults that intercept a secret message.
	Traffic Analysis	An assault that examines the communication styles among entities in a system.
	Location Disclosure	Can reveal something about the network structure or the nodes points.

2.2 Types of IDS

The primary purposes of IDSs are to observe hosts and networks, investigate the behaviours of computer systems, make alarms, and react to unusual behaviours. Because they monitor associated hosts and networks, IDSs are typically used near the shielded network nodes[1].

The researchers Hongyu Liu and Bo Lang(2019), broadly classify the IDS types into two major categories. Based on the data source IDS types and based on the detection techniques IDS types [1]. Figure 3 below shows that the detailed classification of IDS types.

Detection based IDS types: In this type of IDS, attacks are identified based on the signature and anomaly approaches used to detect the attacks. In signature-based[26], IDS system was monitoring the network and identified the attacks with the predefined signature samples. It is also treated as a misuse detection method. The benefit of this approach is a low false alarm rate, the efficiency increase with high signature data samples. The drawback, only known attacks can identify; it leads to high missed alarm rate[1,7]. Anomaly-based IDS types: In this, prepare a standard behaviour profile and unusual behaviours by their degree of variation from the standard profile[26]. The advantage of this approach is to identify the unknown attacks. The pitfall of this method is less false alarm rate[1,7].

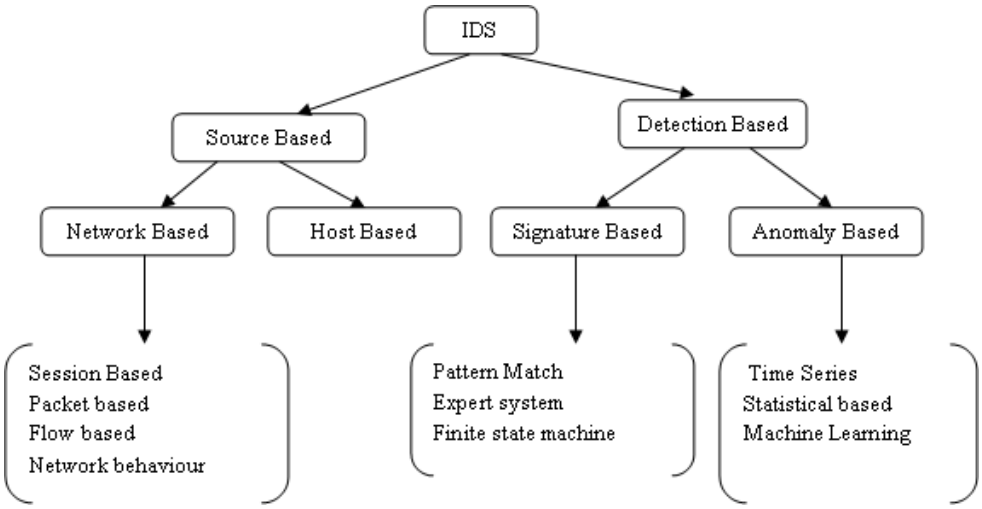


Figure 3: Various IDS Types [1].

2.3 Performance Evaluation Metrics

The best fit machine learning techniques for IDS application, from tested various methods. Need to check performance measure among all methods, this can achieve with performance metrics.

The purpose of performance metrics as follows

- Ranking machine learning algorithms.
- Select the one algorithm over the other.
- Compare all algorithms.

Table 2 shows below about confusion matrix, most accessible metrics used to find accuracy and correctness when the output can be of two or more class labels.

Table2: Confusion Matrix

		Actual	
		Positive	**Negative**
Predicted	**Positive**	**TP**	**FP**
	Negative	**FN**	**TN**

True Positive (TP): TP class, where the original class of the data sample is true and forecasted sample also true.

True Negative (TN): TP class, where the original class of the data sample is false and forecasted sample also true.

False Positive (FP): TP class, where the original class of the data sample is false and forecasted sample also true.

True Positive (FN): TP class, where the original class of the data sample is true and forecasted sample also false.

The various metric checks the performance of machine learning algorithms derived from the confusion matrix, as shown in Table 2[1,2].

Table3: Performance Evaluation Metrics

S NO	METRIC	DESCRIPTION	FORMULA
1	Accuracy	A portion of correctly predicted out of total classes	∑(TP,TN) / ∑(TP,TN,FP,FN)
2	Precision	The ratio of TP vs sum o TP and FP	TP/∑(TP, FP)
3	Recall	Sensitivity measures the proportion of actual positive that are correctly identified	TP/∑(TP, FN)
4	Specificity	Proportion of actual negative that are correctly identified	TN∑(TN, PN)
5	F1 Score	Harmonic average of Precision and Recall	(2*Precision* Recall)/ (Precision + Recall)

3. Datasets Analysis

3.1 KDD Cup 99:[4,5]

The first benchmark dataset for the IDS was KDD Cup 99 dataset, evaluated at MIT's Lincoln Lab and funded by DARPA during International Knowledge Discovery and Data Mining Tools Competition in the year1998-99.

The characteristics of KDD-99 dataset as follows,

i. Provided five target classes to classify the intrusion attacks, the classes are U2R, R2L, Probe, DoS and Normal.

ii. Each pattern with 41 characteristics, comes under any categories like Basic, Traffic and Content.

iii. KDD cup 99 datasets, most of the data belongs to Normal and Daniel of Service categories with 98.61% that is in skewed nature towards only two classes.

iv. The Size of KDD's training dataset contains 4,898,431 samples points, and test dataset contains 2,984,154 samples. In both train and test datasets with large redundant data samples available. The unique data samples of training with 1,074,992 and test 311,029 samples.

The disadvantages with KDD 99 dataset, its oldest dataset almost 20 years back prepared. It may not well suited for a present security context.

3.2 NSL- KDD[5]

The KDD Cup suffered from the redundancy of data, more skewed towards few classes, chance of high false alarms. These all are handled by NSL-KDD dataset.

The following improvement is made in NSL-KDD over KDD-99.

i. Removed the redundancy in training and test datasets, to avoid the biasing towards few classes.

ii. Unnecessary parameters are reduced in the dataset.

iii. In NSL-KDD, train and test sets with reasonable records are available to do the classification., no need of a random sample.

This dataset also has an issue like non-representation of low footprint attacks.

3.3 UNSW-NB15 [5]

IXIA PerfectStorm tool used by Cyber Range Lab of the Australian Centre for Cyber Security in 2014 and named new dataset called as UNSW-NB15.

The characteristics of UNSW-NB15 dataset as follows

i. The number of target classes is 10, namely: Normal, and nine anomalous, namely: Shell Code, Exploits, Generic, Backdoors, Analysis, Fuzzers, Reconnaissance, DoS and Worms.

ii. The increase in target classes compared to KDD 99 and with high Null error rate, the classification accuracy increased.

iii. The train set with 175341 samples and test set with 82332 samples without redundant records.

iv. It contains 47 features, with five groups, namely Flow, Basic, Content, Time, and Additionally Generated.

Many researchers are working with different deep learning algorithms to identify the intruders or attacks in the network. The benchmark datasets, namely KDD99, NSL-KDD and UNSW-NB15, are used to classify the type of attacks. Many researchers worked with any of these datasets to predict the attack class using deep learning algorithms. In this study, we are done the extensive review of these three datasets attack classification performances using DL approaches by the researchers.

To examine the review of various DL methods, an investigation was taken place. In the analysis, we are taken the all benchmark datasets, namely; KDD 99, NSL-KDD and UNSW-NB15 dataset were used (for training and testing data set). We compared the performance analysis of Decision Tree, Logistic Regression, Naive Bayes, ANN, and XGBoost.

4. Systematic Review of DL approaches for IDS

Traditional machine learning algorithms able to handle the structured data with more size. These are not scalable to a large dataset. Their validation efficiency unusually compares with the size of training data. Present circumstances data coming in the different formats and time to time in the network, it increased massively in size. The conventional machine learning methods may not scalable to detect Intrusion attacks[9].

4.1 DL Techniques:

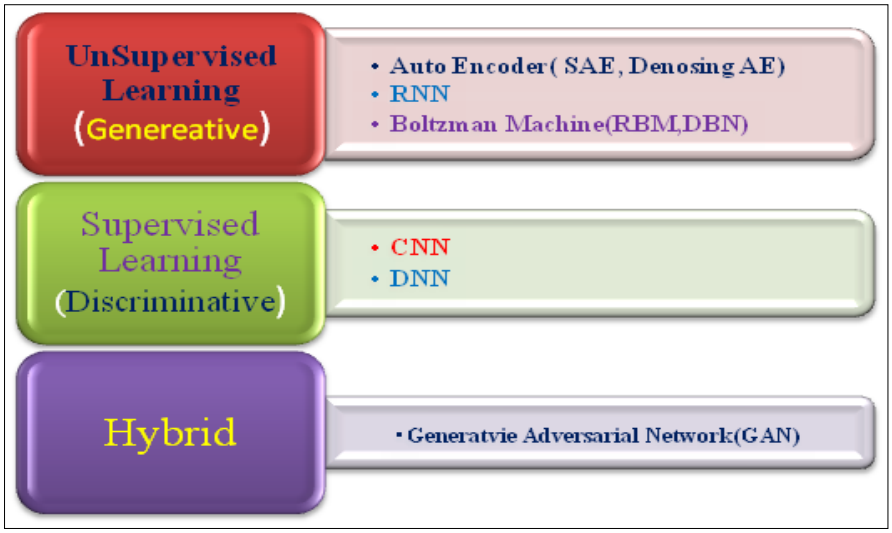


Figure 4: Deep Learning Methods Classification based on the working mechanism

Discriminative or Supervised learning:

When a model learns from sample data, and related goal responses which may consist of numerical data or categorical data or string data, such as labels, in order to eventually determine the appropriate answer when presented with new instances falls under the Supervised Learning classification. The method is under the guidance of an instructor, similar to the human experience. The instructor gives clear examples for the student to memorise, and instead, the student extracts core concepts from those specific examples.

Generative or Unsupervised learning:

Whereas when a model learns from simple examples with no respondent representing, it leaves the technique alone to evaluate the data patterns. This method essentially tries to reorganise the information into something different, such as additional features that may reflect a class or a new set of uncorrelated values. These are very helpful in offering insights into the importance of data and developing practical contributions to supervised machine learning algorithms for humans. As a kind of thinking, it parallels the methods employed by humans to work out that certain objects or things are of the same class, for example, by analysing the measure of the correlation between objects. Many recommendation systems in the context of marketing automation which you see on the web are focused on this sort of learning.

Auto-Encoder (AE):

An AE is a profound neural system presented by Holden et al. [1], commonly utilised for dimensionality reduction by delivering preferable information portrayal over the crude information input. An AE comprises of input and output layers with an equivalent number of highlight vectors, notwithstanding a hidden layer with low-dimensional feature representation. An AE consolidates an encoder and decoder and trains them together utilising backpropagation. The encoder extricates the crude highlights and learns the data representation by changing over the contribution to low-dimensional reflection. At that point, the decoder gets the low-dimensional representation and remakes the first features [15,11].

SAE: More than one hidden layer is fell to develop a deep network and structure the SAE. Features are found out continuously inside and out to develop another data representation [3,11].

Sparse AE: The hidden units in sparse AE have sparsity limitations. The AE stays valuable for learning information portrayals regardless of whether there are many concealed units. Sparsity requirements plan to create low normal yield by making countless neurons latent more often than not [16,11].

De-noising AE: The standard of de-noising is the utilisation of ruined information as a contribution to delivering is fined data representation, where the hidden layers utilise just strong feature vectors [5,11].

Restricted Boltzmann Machine (RBM)

The Boltzmann machine s a unidirectional model proposed by Smolensky in 1986 to tackle issues emerging from the multifaceted nature of BM. The rule behind RBM is to dispense with the associations among neurons in a similar layer. RBM comprises of a noticeable layer for the underlying input variables and a hidden layer holding inactive variables. Every unit in the noticeable layer is associated with all units in the hidden layer with related loads. The hidden units take in the element dispersion from input factors [6,11].

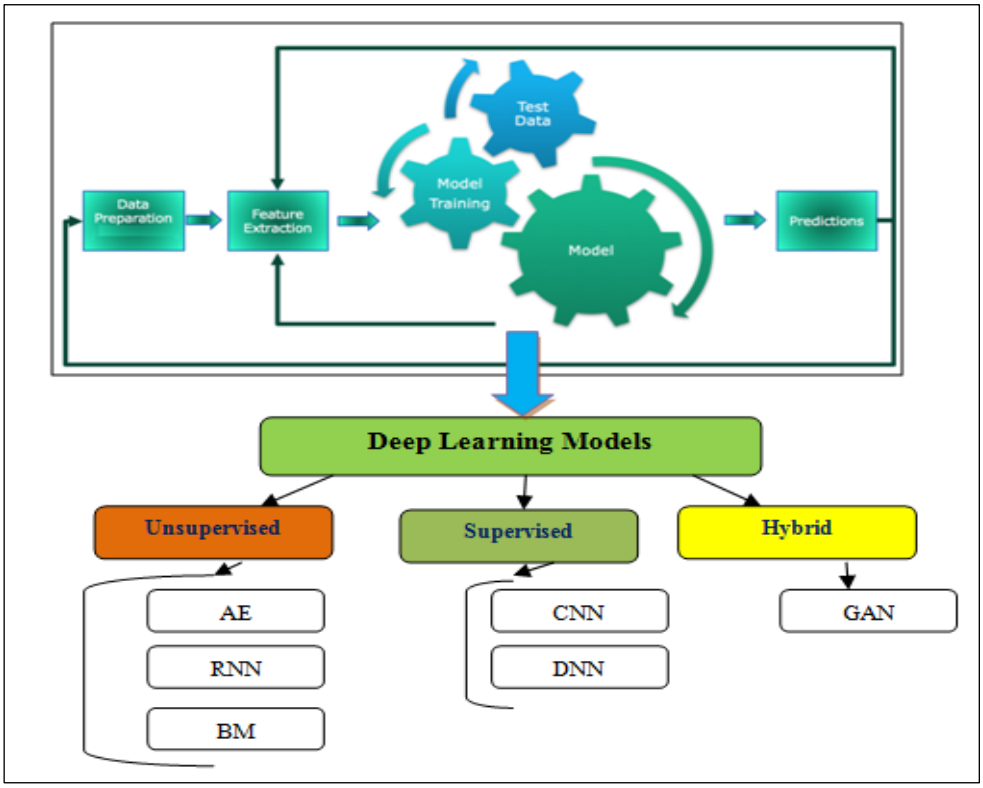
Deep Belief Network (DBN)

A deep belief network (DBN) is made out of stacked RBMs, which are prepared in a greedy layer-wise design. Each RBM is prepared on the head of the past one, where each hidden layer of an RBM is viewed as a contribution to the following RBM. This preparation system brings about a productive and quick deep learning algorithm [7,11].

Recurrent Neural Network (RNN)

An RNN is a powerful feed-forward neural system presented by Hopfield in 1982. It is recognised by its capacity to learn consecutive information after some time steps. In regular feed-forward neural systems, the yield of every unit relies upon the current contribution, with no reliance among input and past yield of a similar unit[11]. In any case, a few applications depend on consecutive information, for example, discourse acknowledgement or time-arrangement information, for example, sensor information, in which each example relies upon the investigation of past examples.

Long short time memory (LSTM): LSTM tackles the vanishing gradient problem issue in vanilla RNN. It can learn long term conditions using the gating mechanism. Each LSTM unit is outfitted with a memory cell that holds old states [8,11].



4.2 Comparative Study

Table 4. below shows the empirical study on various deep learning methods used to predict the intrusions based on the universal datasets for IDS.

Table 4. Performance Evaluation Comparison of IDS using DL methods on various Datasets

CITED	DL Methods Used	Authors	Year	DATASETS		
				KDD	NSL KDD	USNW
				Accuracy	Accuracy	Accuracy
[23]	Auto encoders	XuKui Li, Wei Chen et al.	2020	96.2		
[16]	Intelligent, DNN	R. VINAYAKUMAR, MAMOUN ALAZAB et al.	2019	95 to 99	95 to 99	93.5
[18]	LSTM	Hyeokmin Gwon, Chungjun Lee et al.	2019			82.73
[19]	LuNet CNN, RNN	Peilun Wu and Hui Guo	2019		99.24	97.4
[21]	MLP,CNN, CNN-RNN, CNN-LSTM, CNN-GRU	Vinayakumar R , Soman KP et al.	2017	98.7		
[20]	Random Neural Network	Qureshi, Ayyaz-Ul-Haq et al.	2019		94.5	
[11]	RNN	Marwan Ali Albaha	2019	99.5	97.3	99.9
[13]	RNN	CHUANLONG YIN, YUEFEI ZHU et al.	2017	97.09	94.1	

[22]	Self-Taught Learning (Auto Encoders)	Quamar Niyaz, Weiqing Sun et al.	2015		88.39	
[25]	Autoencoders, RBM, K-Mean	Md Zahangir Alom and Tarek M. Taha	2017	91.86, 92.12		

XuKui Li. et al., used a Random forest to choose the best features, feature group done based on affinity propagation and finally anomaly detection by autoencoders, achieved 96.2% accuracy[23]. R Vinay Kumar. et al. used Intelligent deep neural network to identify the attacks. They used NLP concepts to process and analyse the system calls, to handle the larger dataset using scalable hybrid IDS AlertNet(SHIA) with five layers of DNN achieved 95 to 99 % accuracy on KDD, NSL-KDD dataset and 93.5 % accuracy on UNSW dataset[16]. Hyeokmin Gwon et al. used LSTM with an accuracy of 99%, And also suggested that model compatible with the embedded system and IoT [18]. Peilun Wu and Hui Guo worked with NSL-KDD and USNW datasets with 99.24 and 97.4 % accuracy. They used LuNet with the combination of RNN and CNN to achieve excellent efficiency [19]. Vijayakumar R, Soman KP, Prabaharan Poornachandran used various hybrid combinations of CNN, RNN, LSTM and GRU. The combination of CNN 3 layers with LSTM model achieved 98.7% accuracy[21]. Qureshi et al., in 2019, they worked on binary classification on NSL KDD with Random NN model trained using gradient descent, it given 94.5% accuracy[20]. In the same year researcher, Marwan Ali Albaha came up with RNN-SDR model with less number of features and implemented model on all three benchmark datasets. The proposed mode Self Defence Network achieve good accuracy with 99.5% on KDD99, 97.3% on NSL-KDD and 99.9% on UNSW datasets. The model has three layers as flow collector, anomaly detector and anomaly mitigator[11].

In 2017, CHUANLONG Yin et al. used a bidirectional RNN model and worked on both binary and multiclass classification. The accuracy achieved 97.09% and 94.1 % on KDD99, NSL-KDD dataset respectively. He concluded his model is suitable for NSL-KDD dataset on multiclass classification [13]. Quamar Niyaz et al., in 2015, self-taught learning model with the help of autoencoders on NSL-KDD dataset and gained 88.39% accuracy. In the STL model, two levels, such as unsupervised feature learning on unlabeled data and classification on labelled data[22]. In 2017 the researchers Md Zahangir Alom and Tarek M. Taha worked with Autoencoders, RBM, K-Mean as a combination and achieved 91.86% of accuracy with 92.12% detection rate. AE and RBM are used to extract the features, and iterative k-means clustering is used for final detection of attacks [25].

Gozde Karatas et al., in 2018, investigate on IDS with standard datasets and also worked out recent dataset called CIC IDS 2018. as per there study, DL has emerged as a novel strategy which facilitates the use of Big Data with low training time and high accuracy rate with its unique learning mechanism[12]. Kwangjo Kim et at., in 2017, reviewed supervise and unsupervised DL methods Auto Encoder(AE), Boltzman Machine(BM), and CNN. Their findings, Stacked AE used to extract the features from the dataset with lesser complexity. They suggested that IDS for IoT environment such as CAN used by the unmanned vehicle[14].

Arwa Aldweesh et al., in 2019[15], surveyed supervised, unsupervised and hybrid models of Dl on KDDCup99 and NSL-KDD datasets. AE, RNN and DBN models used earlier. Ensemble and hybrid architectures remain inadequately examined and need to investigate. Muhamad Erza Aminantoa and Kwangjo Kimb in 2017, based on their findings, suggested the combination of supervised and unsupervised learning consistently provide better detection results. They worked on NSL-KDD dataset[24].

5. Conclusion

Network security is one of the modern-day's main issues. An intrusion detection system is one of the solutions implemented to overcome malicious attacks. In fact, attackers are starting to adapt their methods and tactics. Implementing an approved IDS scheme, though, is often an arduous process. The IDS is developed to include the essential identification strategies to protect the devices in networks that are linked explicitly or indirectly to the Internet. Yet it's actually up to the Network Manager at the end of the day to ensure his network stays free of risk. This will not totally shield Intruders network, but IDS helps the Network Administrator track down the man on the web whose very intent is to bring one's network to a point of a breach and make it vulnerable. Throughout a comprehensive review, we have uncovered different findings and models. Deep learning is frequently used for feature learning in intrusion detection approaches. And also we identified that all models worked out on standard network intrusion dataset namely, KDDCup99, NSL-KDD and UNSW-NB15. The present findings describe that more efforts are required to enhance the current state-of-the-art, given these findings. This survey also lays out several research challenges and future directions. Since the benchmark datasets do not tackle the current advanced status of different types of networks, there is an urgent need to use and generate more recent datasets and real-time prototypes based on existing hardware advances..

References

1. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Appl. Sci. 2019, 9, 4396.
2. Lee, Brian; Amaresh, Sandhya; Green, Clifford; and Engels, Daniel (2018) "Comparative Study of Deep Learning Models for Network Intrusion Detection," SMU Data Science Review: Vol. 1: No. 1, Article 8.
3. Chouhan, N., Khan, A., & Haroon-ur-Rasheed. (2019). Network anomaly detection using channel boosted and residual learning based deep convolutional neural network. Applied Soft Computing, 105612. DOI:10.1016/j.asoc.2019.105612
4. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), 18–31. DOI:10.1080/19393555.2015.1125974
5. Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018). Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives. 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS). DOI:10.1109/cccs.2018.8586840
6. Shahid Anwar et.al. From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions, Algorithms 2017, 10, 39; doi:10.3390/a10020039
7. Tiwari, Mohit & Kumar, Raj & Bharti, Akash & Kishan, Jai. (2017). INTRUSION DETECTION SYSTEM. International Journal of Technical Research and Applications. 5. 2320-8163.
8. Pawar, M. V., & Anuradha, J. (2015). Network Security and Types of Attacks in Network. Procedia Computer Science, 48, 503–506. DOI:10.1016/j.procs.2015.04.126
9. Sekhar C.H., Rao K.V. (2020) A Study: Machine Learning and Deep Learning Approaches for Intrusion Detection System. In: Smys S., Senjyu T., Lafata P. (eds) Second International Conference on Computer Networks and Communication Technologies. ICCNCT 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 44. Springer, Cham
10. Dash, T. A study on intrusion detection using neural networks trained with evolutionary algorithms. Soft Comput 21, 2687–2700 (2017). https://doi.org/10.1007/s00500-015-1967-z.
11. Albahar, M. A. (2019). Recurrent Neural Network Model Based on a New Regularization Technique for Real-Time Intrusion Detection in SDN Environments. Security and Communication Networks, 2019, 1–9. DOI:10.1155/2019/8939041
12. Karatas, G., Demir, O., & Koray Sahingoz, O. (2018). Deep Learning in Intrusion Detection Systems. 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). DOI:10.1109/ibigdelft.2018.8625278.
13. 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.
14. K. Kim and M. E. Aminanto, "Deep learning in intrusion detection perspective: Overview and further challenges",2017 International Workshop on Big Data and Information Security (IWBIS), Jakarta, 2017, pp. 5-10, DOI: 10.1109/IWBIS.2017.8275095.
15. Aldweesh, A., Derhab, A., & Emam, A. Z. (2019). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 105124. DOI:10.1016/j.knosys.2019.105124
16. R, V., Alazab, M., KP, S., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 1–1. DOI:10.1109/access.2019.2895334

17. Kim, K., Aminanto, M. E., & Tanuwidjaja, H. C. (2018). Network Intrusion Detection using Deep Learning. SpringerBriefs on Cyber Security Systems and Networks.
18. Gwon, Hyeokmin & Lee, Chungjun & Keum, Rakun & Choi, Heeyoul "Henry. (2019). Network Intrusion Detection based on LSTM and Feature Embedding.
19. P. Wu and H. Guo, "LuNet: A Deep Neural Network for Network Intrusion Detection," 2019 IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 2019, pp. 617-624, DOI: 10.1109/SSCI44817.2019.9003126.
20. Qureshi, A.-U.-H., Larijani, H., Ahmad, J., & Mtetwa, N. (2018). A Novel Random Neural Network Based Approach for Intrusion Detection Systems. 2018 10th Computer Science and Electronic Engineering (CEEC). DOI:10.1109/ceec.2018.8674228
21. R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, 2017, pp. 1222-1228, DOI: 10.1109/ICACCI.2017.8126009.
22. Ahmad Javaid, Quamar Niyaz, Weiqing Sun, Mansoor Alam," A Deep Learning Approach for Network Intrusion Detection System", http://dx.doi.org/10.4108/eai.3-12-2015.2262516.
23. Li, X., Chen, W., Zhang, Q., & Wu, L. (2020). Building Auto-Encoder Intrusion Detection System Based on Random Forest Feature Selection. Computers & Security, 101851. DOI:10.1016/j.cose.2020.101851
24. Aminanto, E., & Kim, K. (2016). Deep Learning in Intrusion Detection System: An Overview.
25. M. Z. Alom and T. M. Taha, "Network intrusion detection for cybersecurity using unsupervised deep learning approaches," 2017 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, 2017, pp. 63-69, DOI: 10.1109/NAECON.2017.8268746.
26. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18–28. doi:10.1016/j.cose.2008.08.003.
27. He has about 50+ research papers in various International Journals
28.