AI Based Techniques For Network-Based Intrusion Detection System: A Review

Yudhir Gala [1], Nisha Vanjari [1], Dharm Doshi [1] and Inshiya Radhanpurwala [1]

[1] *K. J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai, 400022, India*

Abstract

The internet has unlocked a whole new universe. It has no bounds and provides individuals with tremendous economic prospects all throughout the world. People can live better lives as a result of it. The internet has become one of the most important channels for communication. It has caused a massive range of information to be available online. This in turn has led to a lot of new threats coming into play, making it hard for network security to find breaches. An intrusion detection system (IDS) is a technology that scans network activity for unusual behavior and sends out alerts when it is found. It still has trouble detecting new intrusions, increasing the detection's precision and lowering false alert rates, despite the enormous efforts of the researchers. This research paper begins with a quick overview of IDS and its forms. We then go over several AI-based methods for Network-based IDS (NIDS), contrasting their advantages and disadvantages, while also determining evaluation metrics for each. Further discussing the various datasets used. We conclude our research by listing the research challenges along with the current and future trends.

Keywords

Network Intrusion Detection, Anomaly Detection, Deep Learning, Machine Learning

1. Introduction

Cyberattacks are the most devastating and destructive form of modern warfare without weapons, resulting in the disclosure of sensitive personal and business data, disruption of critical operations, ongoing vulnerabilities, and unauthorized and illegal access to devices and software, all of which have a devastating impact on the economy of the nation [21]. These cyberattacks must be avoided. Intrusion-based cyberattacks are now commonplace, and early detection is critical. Currently, an IDS is still a must-have for protecting critical networks from outside intrusions[24].

An IDS is a device that keeps an eye on networks and guards against intrusion by examining network traffic and ensuring its confidentiality, integrity, and availability. Recently, many strategies have been used to effectively identify intrusions across the network. IDS can be broadly divided into two categories based on its deployment method and detection method. Both host-based and network-based IDS can be used as the deployment method. Host-based IDS are made to monitor both network traffic and computer activity, whereas network-based IDSs are simply made to monitor network traffic. The two types of detection method-based IDS are signature-based and anomaly-detection IDS. Anomaly-based IDS is used for detecting changes in behavior, while signature-based IDS is used for risks we are previously aware of[25]. It attempts to identify intrusions by comparing incoming network traffic with known assaults, which are contained in the database as patterns or 'signatures'. IDS does a good job at conventional attacks, but it is ineffective against newer and unobserved attacks.

Researchers have developed a variety of ML and DL based solutions over the past ten years to improve the effectiveness of NIDS in identifying malicious endeavors. The tremendous growth in web traffic and the ensuing security risks, however, have made it difficult for NIDS systems to effectively identify hostile intrusions. In order to use NIDS to accurately identify network attackers, there is still a

[1]ICECI-2023: International Conference on Emerging Computational Intelligence, February 11-12, 2023, Aligarh, India
EMAIL: yudhir.gala@somaiya.edu (A. 1); nvanjari@somaiya.edu (A. 2); dharm.doshi@somaiya.edu (A. 3); inshiya.r@somaiya.edu (A. 4)
ORCID: 0009-0005-3622-1045 (A. 1); 0000-0002-4975-4319 (A. 2);

need for research into this technology. The research study on using DL methods for NIDS is still in its initial phases.

This paper's main goal is to give a comprehensive review of current trends and developments in ML and DL-based NIDS solutions. Our article's primary contributions are: (a) To choose and meticulously study journal articles concentrating on various ML and DL-based NIDS that were published recently (2018-2022). (b) We thoroughly examined each publication and evaluated its different aspects, including its suggested framework, points of strength and weakness, assessment methods, and datasets used. (c) On the basis of these findings, we reported the most current developments in the use of AI methods for NIDS, highlighted numerous difficulties in ML/DL-based NIDS, and provided many future prospects in this significant area.

The rest of the paper is organized as follows: Section II discusses the methodology adopted for literature review. Section III provides an overview of AI Based methods for network intrusion detection. Section IV presents different ML techniques employed for intrusion detection. Section V presents different DL techniques applied for intrusion detection. Section VI gives an overview of the benchmark datasets used by the proposed models. Section VII presents the different evaluation metrics methods used and comparison study of the different methods proposed. Section VIII presents the discussion and analysis based on the literature review of the papers. Ultimately, in section IX, the conclusion of the review is presented.

2. Methodology

2.1. Search Engine Query

The online databases IEEE Xplore, ACM Digital Library, ScienceDirect Elsevier, Wiley Online, and the Scopus indexing database were all searched using the following search query.

Title: (“network intrusion”) AND Keyword: (“machine learning” OR “deep learning”) AND Full Text: (“intrusion detection” OR “anomaly detection”)

2.2. Selection Criteria

The inclusion of papers was determined by two stages: a review of the title and abstract, and a review of the entire paper. Papers whose main goal was to develop new and innovative AI-based techniques for detection against unwarranted invasion were included. Papers were included if they have been printed during the previous five years in conference proceedings and peer-reviewed journals in the English language. Over 51 raw results were gathered based on the search engine query. After the first stage, only 34 papers were selected. After the second stage of the selection criteria, only 25 papers were selected based on the conditions mentioned above.

3. Overview Of AI Based Methods

In the last two decades, network intrusion detection has been implemented using AI based methods. These methods are implemented in three phases; the first phase is data preprocessing phase which includes techniques like encoding, normalization and feature extraction being conducted on the datasets. The second phase is the training phase where a major portion of the preprocessed data is used to train the models. The third phase is the testing phase where the trained model is tested on an unseen portion of the dataset and the model is evaluated based on various performance metrics. The following sections discuss different ML/DL based approaches for network intrusion detection.

3.1. Support Vector Machine, Isolation Forest Algorithm & Naive Bayes

SVM is used to address classification and regression problems. The SVM algorithm seeks to identify the best hyperplane that may partition n-dimensional area into classes in order to quickly classify fresh data points. SVM is used to choose the extreme vectors and points that contribute to the hyperplane. Chen et al [13] employed CNN to a NIDS model, for the task of feature extraction and its output was given as input to the SVM for the classification and PSO algorithm finetunes the RBF kernel and penalty coefficient of the SVM. The model gave an accuracy of 94.5% on the NSL-KDD dataset [31].

Isolation forest is a ML technique used to uncover abnormalities. The system uses unsupervised learning to isolate outliers in the data to look for anomalies. By randomly selecting a feature from the available features and dividing the value between the highest and lowest values of that feature, it is able to identify the outliers. The anomalous data points will be different from the rest of the data by having shorter paths in the decision tree as a result of the random feature partitioning. Chiba et al. [1] suggested an intrusion detection framework involving a hybrid approach. Suricata and Isolation Forest algorithms were used in a layered manner. The proposed framework claims to work on a smaller sample size and is based on unsupervised learning. By proposing a hybrid framework of signature and anomaly based IDS , it provides a solid line of protection against attacks in the network.

Naive Bayes is a method for classifying system problems with binary and many classes. The concept is fairly easy to comprehend when it is described using binary or categorical input data. Wisanwanichthan et al. [5] presented a framework using an ensemble of Naive Bayes and SVM. This paper can identify attack classes of low frequency like U2R and R2L with high detection accuracy of 96.67% and 100% respectively. The proposed model for training purposes divides the dataset into two groups , one group which has all the data and another group which contains the classes of normal data and low frequency attacks like U2R and R2L. Both groups undergo data transformations like Intersectional Correlated Feature Selection, one hot encoding and PCA. The Naive Bayes algorithm is trained on the first group and the SVM is trained on the second group. The model takes on a layered approach for intrusion detection ,hence increasing its efficiency and reliability. The NSL-KDD [31] dataset was used for the assessment of the model and has a 93.11% overall detection rate.

3.2. Autoencoders (AE)

Different types of AE have recently been applied to NIDS in order to consistently and speedily identify unidentified attack kinds while also easing the strain of the taxing labeling operation. AE is essentially an unsupervised artificial neural network that tries to encode data by compressing it into smaller dimensions and then decoding the data to recreate the original input. It takes a lot of time and effort to identify the ideal model architecture and hyperparameter values of the AEs that produce the best detection performance, despite the fact that the AEs are effective in detecting new sorts of attacks. This could be a barrier to the use of AE-based NIDS in actual applications[20].

To properly identify abnormal traffic, Gharib et al. [4] suggested a semi-supervised DL technique. It employs two AEs in a cascading fashion to detect anomalies in communication networks. The fundamental idea here is to decide on the numerous incoming network flows in two distinct phases, with a different AE performing detection in each step. The proposed model generated an accuracy of 96.45% along with f1-Score of 96.49%, precision of 95.56% and recall of 97.43% upon being evaluated exhaustively utilizing the NSL-KDD [31] dataset. Christopher et al. [9] proposes a method that detects anomalies in computer data streams, and it gives lower running time and cost of labeling contrasted to traditional models. For UNSW-NB15 [32] dataset, the model generated 79.1% as accuracy and 70.3% as f1-score and had a runtime of 20.6 seconds, whereas the KDD99 dataset [30] generated an accuracy of 98% along with f1-score of 81.2% and had a runtime of 25.3 seconds. The research [6] suggests a real-time anomaly detection method that builds AEs out of memristor crossbars. In neuromorphic systems, memristors are often used to simulate the idea of synaptic connection. Memristors could therefore be utilized to record the degree to which a neuron is connected to each of its incoming

connections. Using the NSL-KDD dataset, this system was capable of distinguishing between normal and attack data with accuracy of 92.9%.

In ensemble learning, the predictions from various base detectors are combined by ensemble learning algorithms to produce more reliable results. Therefore, the variance of the model is decreased by using numerous model executions and using a central estimator of the scores. The paper [7] proposed an ensemble method based on stacked generalization principle, using DNN and LSTM as base models and logistic regression as the meta model. The preprocessed data that had undergone dimensionality reduction using sparse AE is used for training the meta-classifier. This procedure improves the detection rate of network anomalies. The efficiency of the method is tested on datasets NetML-2020 [28], LITNET-2020 [29] and IoT-23 [22]. The IoT-23 generated an accuracy of 99.7% along with an F1-Score of 98%, Precision of 100% and recall of 95%, whereas the LITNET-2020 generated 100% as overall detection accuracy, 100% as F1-score, Precision and Recall of 100%, and ultimately the NetML-2020 generated an overall accuracy rate and F1-score of 100% along with an precision and recall of 99%.

Mirsky et al. [8] proposes Kitsune which is an adaptive NIDS that learns to detect intrusion and anomalies on the network in real time. It is based on unsupervised learning and shows efficiency in the task of network intrusion detection. It presents an ensemble of AEs that work effectively together to discern between normal and abnormal traffic patterns. This paper demonstrates the pragmatic and economic efficiency of Kitsune. Another paper [11] proposes a NIDS model based on an ensemble of traditional AEs. In this paper, the data preprocessing step employs the recursive feature addition algorithm for feature reduction which effectively reduces the training time of classifiers. The system uses NSL-KDD [31] and CSE-CIC-IDS-2018 [36] datasets. Based on the analysis of the results, it is seen that the proposed system works in the way that when the attack classes have similar statistical features to normal data, it has difficulty in differentiating the two classes and hence suffers from low detection rate for such attacks. Yang et al. [21] proposed Griffin which performs network intrusion detection in real time through the ensemble of AEs in Software defined Networks. The anomaly detection was done by training the ensemble of AEs on the sub instances and categorizing attacks by using RMSE as an anomaly threshold. It was trained on mirai active wiretap dataset and other open datasets. The proposed model realizes a 19% improvement of AUC and achieves 40% lower complexity when compared to the other existing methods.

3.3. Long Short Term Memory (LSTM)

In tasks involving sequence prediction, several recurrent neural networks (RNNs) are efficient in comprehending long-term dependencies. Since LSTM utilizes feedback connections, the complete data collection is processed, with the possible exception of single data items like images. In the paper [18], Hierarchical LSTM model was implemented that can learn from many layers of temporal hierarchy while dealing with complicated data flow sequences. By weighting the loss function, it addresses the imbalance in the NSL KDD [31] dataset and prevents the classifier from learning the majority of the representative classes. It produced an accuracy rate of 83.85% on the dataset.

Deore et al. [19] presented Deep LSTM algorithm optimized using Chimp Chicken Swarm Optimization-based algorithm along with CNN feature extraction capabilities to help with effective intrusion detection. Benchmark datasets used are NSL KDD [31] and BotIoT datasets. The model generated 99.17% as accuracy , 99.94% as specificity, and 98.60% as sensitivity. Amutha et al [14] proposed a deep RNN using LSTM algorithm which gave maximum accuracy with less number of iterations and less memory usage when compared with the methods mentioned in their paper.

3.4. Extreme Learning Machine (ELM)

ELM [37] is a novel type of single hidden layer feed forward neural networks that differs from conventional learning methods. For classification, regression, clustering, compression, and feature

learning, these neural networks with a single or multiple layers of hidden nodes are used. ELMs are thought to be able to learn tens of thousands of times more quickly than networks trained using the backpropagation method. Jingyi et al [15] suggests a unique detection method for network attacks using ELM and Supervised Locality Preserving Projection (SLPP). The SLPP algorithm extracted the features from the KDD Cup '99 [30] dataset and the extracted features are used to build and train the ELM classification model. Various feature extraction methods like PCA,FDA and LPP are compared. The model received an accuracy of 99.29% for detecting normal packets, 98.68% for detecting DoS attacks, 98.73% for detecting Probe attacks, 96.35% for detecting U2R attacks and 99.84% for detecting R2L attacks.

3.5. Convolutional Neural Network (CNN)

A class of DNN called CNN is most frequently used to evaluate visual imagery. It makes use of a unique method called convolution. These neural networks are made up of numerous artificial neuronal layers. Network intrusion detection has also seen use cases for it. Xiao et al. [32] suggests the use of CNN-based IDS. First, the network traffic data is stripped of its superfluous and unnecessary attributes using a variety of dimensionality reduction techniques. With the use of this neural network, features from the reduction data are automatically extracted, and supervised learning is utilised to automatically extract data that is better for identifying incursion. Utilizing a common KDD99 [30] dataset to assess the effectiveness of the model, the reviewed proposal converts the authentic traffic vector format into an image file format to lower the required computational resources. The experiments' results demonstrate that the CNN-IDS model put forth in this paper effectively detects network intrusion data through dimensionality reduction. Recall and accuracy are both capable of reaching a maximum of 94.0% and 93.0%, respectively, via the suggested approach.

3.6. Generative Adversarial Networks (GAN)

A semi-supervised model is presented by Jeong et al. [12] for intrusion detection that utilizes only ten labelled data per each flow type and huge amount of unlabelled data during training, hence solving the problem of supervised learning approach which requires labeled datasets that are hard to acquire. The model uses DCGAN which traines the discriminator on the unlabelled dataset as well as the fake data generated by the generator and then it is transferred by the CNN that is trained on only 10 labeled data of each type. The benchmark dataset used was CIC-IDS-2017 and the model gave an accuracy of 88.7%. Nie et al. [17] proposes a system for securing Social IoT based edge networks using GAN. The detection algorithm based on GAN is trained targeting a single attack and then several intrusion detection models targeting every singular attack are combined to create an ensemble to detect multiple attacks. By being trained and taught about known attack types, this model can recognise novel attack types. It gave an accuracy of 95.32% on the CSE-CIC-IDS2018 [36] dataset and 98.53% on the CIC-DDOS2019 dataset.

Table 1
Comparison of Models Based on Strength and Weakness

Study	Strengths	Limitations
Zouhair Chiba et al. [1]	The model works on a smaller sample size and utilizes unsupervised learning methodology. The NIDS framework uses Suricata. It has a hybrid design and hence provides firm defense against network intrusion attacks.	The proposed framework in the paper has not yet been implemented and therefore cannot be evaluated.
Shone et al. [2]	The proposed model can handle high volumes of inflowing data. It performs effective dimensionality	The proposed model is not trained to handle modern zero day attacks as trained on older

	reduction using stacked AEs. Performs in depth monitoring to increase performance accuracy.	datasets and it has not yet been evaluated on real time network traffic.
Hongli Deng et al. [3]	The addition of noise during the network training phase enables the encoder to understand better features, which improves the durability of the data after reduction. The model may be used with high dimensional and complex network data.	The model uses KDD Cup '99 and it hasn't yet been tested using other datasets and real-time network environment.
Mohammed Gharib et al. [4]	The methodology of using an ensemble of AEs provides the model with a higher and accurate detection rate. The use of Semi-supervised learning technique leads to an increased performance	The model has not yet been evaluated on real time network traffic and other datasets.
Treepop et al. [5]	The proposed model can detect low frequency intrusion classes in the NSL-KDD with great precision.	Due to the fact that two steps are necessary to certify whether a connection is secure, attack detection takes longer and resource usage increases.
Alam et al. [6]	The proposed model provides a method for real time training and requires low power hardware for effective intrusion detection within networks.	The system has a far lower chance of classifying or flagging an attack type as uncommon if it sees it frequently over a period of time.
Vibekananda Dutta et al. [7]	The model uses the latest IOT and modern network based datasets. By utilizing the SMOTE and Edited Nearest Neighbors algorithm for balancing classes in the datasets, it improves the performance of the model in the task of detecting intrusions.	The proposed model has not yet been evaluated on real time network traffic. Ensemble of DL models being used as classifiers may increase the complexity of the proposed system.
Yisroel Mirsky et al. [8]	The proposed model has a small memory footprint. The model also has low computational complexity due to which it can be run on low level hardware. This system employs an adaptive NIDS that can discover network assaults and shows high efficiency in the task of detecting attacks on the network.	The proposed model cannot be trained on real time traffic if proper measures are not taken that make sure only normal packets are being used for training and if hidden attack vectors in the packet flow are trained as normal due to which such anomalies will not be detected.
Christopher Nixon et al. [9]	For computer data streams, the model adopts dropout probability and naive anomaly threshold with decay for effective online learning. The running time and labeling cost is lesser than previous online learning methods.	The model has difficulties in differentiating streams of normal and anomaly data having similar characteristics,
Chun Long et al. [11]	The paper proposes a lightweight model for intrusion detection.It employs the recursive feature method for selecting optimal features from the dataset. The model incorporates AE so that class imbalance problems can be addressed.	The model provides only an appreciable level of accuracy for identifying weakly representative classes in the NSL-KDD dataset.

Hyejeong Jeong et al. [12]	The proposed model is used to solve the supervised manner of learning that requires labeled data which is hard to obtain. The model only needs 10 labeled data per flow type, for training, and the rest can be unlabelled.	The model's performance in identification of minority attack classes is not mentioned.
Liyan Yang et al. [16]	The proposed model involves real time detection and produces high accuracy along with a low latency. The model protects the privacy of the dataset by adding noise to the model parameters.	The model has not yet been evaluated on a real time network environment in order to properly evaluate its advantages of low latency.
Y. Xiao et al. [23]	The proposed CNN-based model has the ability to classify traffic data in addition to choosing characteristics. Convolutional kernels considerably reduce parameters effectively and the size of data needed for training to detect attacks in traffic data.	Any CNN based model requires a massive amount of training data which is a downside.

1.

4. Benchmark Datasets

This section contains information on the prevalent datasets that researchers use to test and evaluate the efficacy of their suggested models.

- NSL-KDD : It [31] has been proposed to address some of the inherent issues with the KDD'99 data set. Additionally, there are 41 features in this dataset. The attacks are similar to the one we see in the KDD Cup '99, they are; Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R) are the four types of attacks.
- UNSW-NB15 : This dataset was produced by the Australian Center for Cyber Security [32]. 49 features are extracted from almost two million data using Bro-IDS, Argus tools, and some newly generated algorithms. The numerous sorts of attacks in this dataset include reconnaissance, worms, port scans, shellcode, generic, DoS, exploits, etc.[33].
- CIC-IDS2017 : It was developed by the Canadian Institute of Cyber Security (CIC) in 2017 [34]. It includes both, recent real-world attacks in addition to typical routines. CICFlowMeter analyzes network traffic using timestamps, source and destination IP addresses, protocols, and attack data. Furthermore, it includes typical attack scenarios including the Brute Force Attack, HeartBleed Attack, Botnet, Distributed DoS (DoS), Web Attack, and Infiltration Attack [35].
- CSE-CIC-IDS2018 : The Communications Security Establishment (CSE) and CIC worked together to create this dataset [36] in 2018. The user profiles that represent the various events in an abstract way are made. The dataset is created by combining each of these profiles with a special set of attributes. Seven distinct attack scenarios are included: DoS, DoS, Botnet, Brute-force, Heartbleed, and Web attacks as well as internal network intrusion [24].
- LITNET-2020 : The senders and collectors in the NetFlow dataset are the same. Cisco routers and Fortige (FG-1500D) firewalls serve as the senders, and data collection, storage, and filtering software serves as the collector [29]. There are 84 feature attributes in the final datasets.Attacks include: Smurf, ICMP, UDP, TCP, SYN, HTTP, LANDattack, Blaster, Code Red, Spam bot detection, Reaper, scanning/spreading, and packet fragmentation attack [27].
- NetML-2020 : 30 network traffic records were provided by Stratosphere IPS for the development of this dataset [28]. The NetML dataset has 48 feature characteristics and 48 flows. At the highest level of granularity, the dataset is binary (benign or malicious), with specific software communication identified at the mid-level. The fine-grained level classifies many different forms of attacks, including Ramit, HTBot, etc.

5. Discussion and Analysis

5.1. Current Trends and Observations

As ML methods cannot perform well on large datasets unless they are labeled, there has been a shift towards adopting DL methods as seen in Fig. 2. DL methods can extract and learn better features from the large datasets. This shift has also been spurred by the advent of GPUs and cloud computing capabilities. Another observation that can be seen is that the majority of the models are being trained and evaluated on datasets like KDD Cup '99 and NSL-KDD. Such datasets represent network traffic data from nearly 20 years ago. Therefore, evaluating the models on these datasets does not properly project their performance on newer modern network traffic data. Nearly 45% of the above proposed models used NSL-KDD and KDD Cup'99 [30] datasets for training and performance evaluation [Fig. 1]. Moreover it is seen that not many proposed systems while training their models are taking into account the problem of class imbalance occurring in various datasets. Therefore less representative classes of the datasets have a much lesser detection accuracy compared to the more representative classes. Hence, the capability of the proposed IDS system to detect anomalies decreases and therefore would not be viable for real world networks. Another major drawback is that the viability of the proposed systems in the real world traffic is not discussed. In order to function properly in a real network, the proposed IDS system will have to deal with throughput and latency issues. Especially, due to the complexity of the DL models there will be massive decrease in the model's performance to detect attacks in the high speed networks where there is a large amount of data being transmitted.

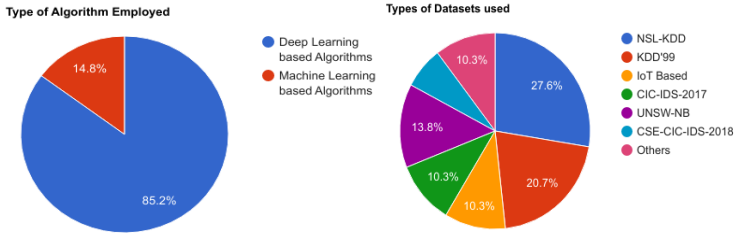

Figure 1: DL and ML models Distribution & Dataset Distribution

Another observation is that not many high performing models are focusing on online learning. In today's computer networks, newer attacks are being seen everyday and adaptability of such models to detect such attacks without offline training is very low. Therefore when proposing systems for network intrusion detection, they should adapt to real concept drift in networks. The majority of the proposed solutions for intrusion detection are using AEs. These have been mainly used for reduction of dimensionality and feature extraction. Then classification tasks are mainly done by ML and DL models. We have also seen an increase in combining different models to create a proposed ensemble method that is being used for network intrusion detection.

5.2. Research Challenges

- Absence of a Systematic Dataset: Many current datasets contain network traffic data which classify only a few types of attacks. The features of every dataset are also very different, therefore the proposed models need to be trained separately on every dataset in order to check their performance metrics. There should be a systematic dataset containing all possible types of attacks related to particular types of networks making it easier for researchers to evaluate the performance of the models.
- Class Imbalance in Datasets: Majority of the recent datasets contain classes which have low representation compared to other classes and therefore many proposed models classes tend to have a low detection accuracy for those minority classes.
- Resources consumed by DL models: Though DL models are better than ML models for training on large datasets and learning important features from the dataset on their own, they are

complex and have high resource consumption tendencies. High latency of packets being transmitted in the network is another problem that the complexity of DL models brings.

- Low Performance in Real time environment: Many models suffer from this challenge, as the models are being trained on older datasets and therefore do not perform as well as in lab environments. Therefore, proposed models should be tested on real time traffic data to access its performance in modern networks.

5.3. Future Trends

- Unsupervised and Semi Supervised Learning Approaches: As the relevant labeled datasets are becoming more and more difficult to obtain, unsupervised and semi supervised approaches are becoming the way to train models for the researchers. These methods also help make online learning models more prevalent and increase their adaptability to changing modern networks .
- Lightweight and Distributed IDS: With the advent of IoT devices and edge computing, the distributed networks containing sensor nodes having limited computational power and memory are becoming more prevalent. Hence, the concept of lightweight IDS that are distributed over different sensor networks that has effective intrusion detection capabilities needs to be designed and researched.
- Hybrid Approach: Another future trend is employing DL model for feature extraction and ML model for classification. This hybrid approach will help reduce the complexity of the systems. Another approach can be integrating anomaly based IDS with the signature based IDS in order to solidify network defense capabilities by utilizing the best characteristics of each IDS.

6. Conclusion

With the aim of giving new researchers an overview of the latest research, contemporary trends, and breakthroughs in the domain, this article provides an in-depth examination of network intrusion detection methods based on ML and DL algorithms. Relevant NIDS-related papers which employed different AI methodologies are selected meticulously. A rigorous process is used to choose the pertinent publications in the area of Al-based NIDS. On the basis of the review papers, a detailed explanation of IDS and its numerous classification techniques is presented first. The method used in each article is then discussed, along with its benefits and drawbacks with regard to the model's complexity and intrusion detection capability. This study has revealed a current trend of using DL-based methods to improve NIDS performance and efficiency in terms of accuracy rate and false alarm rate. The analysis also shows that about 50% of the proposed methods were tested on the NSL KDD and KDD Cup ’99 datasets. However, the premise that all these datasets are too outdated to emerging network threats restricts the efficacy of the offered techniques in real-time scenarios. The most recent datasets, such as CSE-CIC-IDS2018, LITNET-2020, and NetML-2020, should be used to evaluate the system in order for the Al-based NIDS techniques to operate more precisely in terms of intrusion detection. We will capitalize this knowledge to develop a novel, portable, and successful hybrid network IDS in the near future that will successfully identify network intruders by integrating unsupervised and semi-supervised learning techniques.

7. References

[1] Zouhair Chiba, Noreddine Abghour, Khalid Moussaid, Amina El Omri, and Mohamed Rida. 2019. Newest collaborative and hybrid network intrusion detection framework based on suricata and isolation forest algorithm. In Proceedings of the 4th International Conference on Smart City Applications (SCA '19). Association for Computing Machinery, New York, NY, USA, Article 77, 1–11.

[2] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018.
[3] Hongli Deng, Tao Yang, "Network Intrusion Detection Based on Sparse Autoencoder and IGA-BP Network", Wireless Communications and Mobile Computing, vol. 2021, Article ID 9510858, 11 pages, 2021.
[4] Gharib, Mohammed, Bahram Mohammadi, Shadi Hejareh Dastgerdi and M. Sabokrou. "AutoIDS: Auto-encoder Based Method for Intrusion Detection System." ArXiv abs/1911.03306 (2019): n. pag.
[5] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," in IEEE Access, vol. 9, pp. 138432-138450, 2021.
[6] Md. Shahanur Alam, B. Rasitha Fernando, Yassine Jaoudi, Chris Yakopcic, Raqibul Hasan, Tarek M. Taha, and Guru Subramanyam. 2019. Memristor Based Autoencoder for Unsupervised Real-Time Network Intrusion and Anomaly Detection. In Proceedings of the International Conference on Neuromorphic Systems (ICONS '19). Association for Computing Machinery, New York, NY, USA, Article 2, 1–8.
[7] Dutta, Vibekananda, Michał Choraś, Marek Pawlicki, and Rafał Kozik. 2020. "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection" Sensors 20, no. 16: 4583.
[8] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. ArXiv, abs/1802.09089.
[9] Christopher Nixon, Mohamed Sedky, and Mohamed Hassan. 2020. Autoencoders: A Low Cost Anomaly Detection Method for Computer Network Data Streams. Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing (ICCBDC '20). Association for Computing Machinery, New York, NY, USA, 58–62. https://doi.org/10.1145/3416921.3416937
[10] J. Lu, H. Meng, W. Li, Y. Liu, Y. Guo and Y. Yang, "Network intrusion detection based on Contractive Sparse Stacked Denoising Autoencoder," 2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2021, pp. 1-6, doi: 10.1109/BMSB53066.2021.9547087.
[11] C. Long, J. Xiao, J. Wei, J. Zhao, W. Wan and G. Du, "Autoencoder ensembles for network intrusion detection," 2022 24th International Conference on Advanced Communication Technology (ICACT), 2022, pp. 323-333, doi: 10.23919/ICACT53585.2022.9728934.
[12] H. Jeong, J. Yu and W. Lee, "Poster Abstract: A Semi-Supervised Approach for Network Intrusion Detection Using Generative Adversarial Networks," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484569.
[13] C. Chen, X. Xu, G. Wang and L. Yang, "Network intrusion detection model based on neural network feature extraction and PSO-SVM," 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP), 2022, pp. 1462-1465, doi: 10.1109/ICSP54964.2022.9778404.
[14] S. Amutha, K. R, S. R and K. M, "Secure network intrusion detection system using NID-RNN based Deep Learning," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752526.
[15] W. Jingyi, G. Xusheng, H. Jieli and L. Shenghou, "ELM Network Intrusion Detection Model Based on SLPP Feature Extraction," 2021 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), 2021, pp. 46-49, doi: 10.1109/ICPICS52425.2021.9524271.
[16] L. Yang, Y. Song, S. Gao, A. Hu and B. Xiao, "Griffin: Real-time network intrusion detection system via ensemble of autoencoder in SDN," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2022.3175710.
[17] L. Nie et al., "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 134-145, Feb. 2022, doi: 10.1109/TCSS.2021.3063538.
[18] H. Hou et al., "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," in IEEE Access, vol. 8, pp. 90907-90913, 2020, doi: 10.1109/ACCESS.2020.2983953.
[19] B. Deore and S. Bhosale, "Hybrid Optimization Enabled Robust CNN-LSTM Technique for Network Intrusion Detection," in IEEE Access, vol. 10, pp. 65611-65622, 2022, doi: 10.1109/ACCESS.2022.3183213.
[20] Song, Y.; Hyun, S.; Cheong, Y.-G. Analysis of Autoencoders for Network Intrusion Detection. Sensors 2021, 21, 4294. https://doi.org/ 10.3390/s21134294
[21] Alom, Md. Zahangir, Venkataramesh Bontupalli and Tarek M. Taha. "Intrusion detection using deep belief networks." 2015 National Aerospace and Electronics Conference (NAECON) (2015): 339-344.

[22] Sebastian Garcia, Agustin Parmisano, & Maria Jose Erquiaga. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746)
[23] Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 42210-42219, 2019, doi: 10.1109/ACCESS.2019.2904620.
[24] Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. Paper presented at: Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP). Madeira, Portugal 2018:108-116
[25] Ahmad Z, Shahid Khan A, Wai Shang C, Abdullah J, Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans Emerging Tel Tech. 2021;32:4150. https://doi.org/10.1002/ett.4150.
[26] V. Kanimozhi, T. Prem Jacob, Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing, ICT Express.
[27] Claise, B.; Sadasivan, G.; Valluri, V.; Djernaes, M. Cisco Systems Netflow Services Export Version 9. Available online: https://www.hjp.at/doc/rfc/rfc3954.html (accessed on 14 August 2020)
[28] Barut, Onur, Yan Luo, Tong Zhang, Weigang Li and Peilong Li. “NetML: A Challenge for Network Traffic Analytics.” ArXiv abs/2004.13006 (2020): n. pag.
[29] Damasevicius, R.; Venckauskas, A.; Grigaliunas, S.; Toldinas, J.; Morkevicius, N.; Aleliunas, T.; Smuikys, P. LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion Detection. Electronics2020, 9, 800.
[30] Bay S. The UCI KDD Archive, Irvine, CA: University of California, Department of Computer Science;
[31] Tavallaee M. Bagheri E. Lu W. Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. Paper presented at: Proceedings of the IEEE Symbom on Computational Intelligence for Security and Defense Applications. Ottawa, ON, Canada: IEEE: 2009:1-6.
[32] Moustata N. Slav lUNSW-NBI5: a comprehensive data set for network intrusion detection systems (UNsw-NBls network dataset). Paper presented at: Proceedings of the Military Communications and Information Systems Conference (MilCIS). Canberra, ACT, Australia: IEEE; 2015:1-6.
[33] Moustafa N. Slay J. The evaluation of network anomalv detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. If Sec J A Global Perspect. 2016;25(1-3):18-31. https://doi.org/10.1080/19393555.2015.1125974.
[34] Lashkari AH, Draper-Gil G, Mamun MSI, Ghorbani AA. Characterization of tor traffic using time based features. Paper presented at: Proceedings of the 3rd International Conference on Information Systems Security and Privacy(ICISSP). Porto, Portugal; 2017:253-262.
[35] Abdulhammed R, Musafer H, Alessa A, Faezipour M, Abuzneid A. Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics. 2019;8(3):322. https://doi.org/10.3390/electronics8030322
[36] Karatas G. Demir O. Sahingoz OK. Increasing the performance of machine learning-based IDs on an imbalanced and up-(o-date dataset IEEE Access. 2020;8:32150-32162. https://doi.org/10.1109/ACCESS.2020.2973219)
[37] Guang-Bin Huang, Qin-Yu Zhu and Chee-Kheong Siew, "Extreme learning machine: a new learning scheme of feedforward neural networks," 2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541), 2004, pp. 985-990 vol.2, doi: 10.1109/IJCNN.2004.1380068.