A Systematic Review on Network Intrusion Detection System based on machine learning and deep learning approach

Anto Jenisha Immastephy A[1], and *Dr. K. Punitha*[2*]

[1]Research Scholar, Department of Electrical and Electronics Engineering, PSR Engineering College, Sivakasi, Tamilnadu
[2]Professor, Department of Electrical and Electronics Engineering, PSR Engineering College, Sivakasi, Tamilnadu.

Abstract. Today's security attacks on computer networks are becoming more complex and severe, which has prompted security researchers to use a variety of machine learning techniques to safeguard the information and reputation of their clients. Detecting network infiltration has long been a difficult task. Machine learning advancements have raised the way for improving intrusion detection systems (IDS). This development has led to intrusion detection's integration into network security. Using supervised machine learning techniques, intrusion detection has attained great detection accuracy. However, it is unlikely that a machine learning (ML) classifier will be able to correctly identify all attacks, particularly obscure ones.An approach based on deep learning is presented for more precise intrusion detection. This review article presents an extensive survey and classification of deep learning-based intrusion detection techniques with an emphasis on these approaches. The main background ideas about the IDS architecture and several machine and deep learning approaches are initially presented. Then, it categorizes these schemes based on the many types of methodologies each one employs. It explains how accurate intrusion detection is achieved through the use of machine and deep learning networks. The researched IDS frameworks are then fully analysed, with final thoughts and suggested directions for the future underlined. **Keywords--Cyber security, Machine learning, intrusion detection, deep learning, anomaly detection.**

1 INTRODUCTION

The extensive growth of computer networks and the new, evolving applications on them have made it possible for attackers to launch a variety of security assaults against them using a variety of techniques. In the past few years, there has been a sharp rise in attacks on computers and network-based services, and as a result, cyber security has become an important subject in protecting systems from threats on a local and worldwide scale. Given their danger, intrusion threats must be immediately addressed. The risk of intrusion is greatest for organizations, particularly those with high security requirements like military bases and airports.

Corresponding author email id- kgpunitha@gmail.com

The fundamental security has been already served by the encryption system in computers networks [2], unrecognized threats continue to exist in various forms and negatively impacted the services as a whole.Based on the intrusion detection behaviour the IDS can be categories into two modes: anomaly detection, and signature detection. Establishing a model for normal behaviour access and classifying behaviours that deviate from this model as intrusions are requirements for anomaly detection. How to define a condition as "normal" is the key to this detection technique. On the other hand, in order to develop a model, signature detection has to compile all potential undesirable and prohibited behaviours. This model-compliant behaviour is deemed to constitute an incursion. This method primarily assesses if the data obtained contains the event characteristics that violate the security policy. The main technique is to keep a knowledge base updated [3].
Artificial intelligence (AI) science known as "machine learning" focuses on how to classify and forecast algorithms using data or prior knowledge [4]. Numerous scholars have utilized the machine learning approaches to network IDS and obtained successful detection results as a result of the advancement of ML technology[5].
The most significant component of the procedure is defining the analysis goals, because the data and models necessary to analyse different intrusion detection (ID) situations will differ. The approach, which is based on a machine learning algorithm, is mostly employed in abnormal IDS. In the prior research several machine learning based algorithms are improved with novel other algorithms and introduced a better defence system [6].
Traditional machine learning methods suffer with a lack of labelled training datasets and rely mostly on human-retrieved attributes, making them difficult to use on big platforms [7]. Artificial neural networks, or ANNs, were principally used to construct the cutting-edge machine learning paradigm known as "deep learning," which outperforms other traditional MLapproaches. Deep learning algorithms can learn through unsupervised, semi-supervised, or supervised manner [8].They gain advantage from the use of hierarchical levels, which, rather than relying on manual characteristics, are intended to recognize appropriate high-level attributes from raw input data. [9], [10]. Deep learning algorithms have lately been applied successfully in a variety of fields. Furthermore, DL has gained a lot of attention in the context of intrusion detection, and the prior studies includes a various form ofDL method based anomaly detection models to handle different types of intrusions and security threats.
In order to provide an overview, investigation, and assessment of modern machine learning and deep learning techniques used in network IDS, this study has chosen to focus on these algorithms.
This paper's key contributions are grouped into the following categories

- This paper proposed the latest development of ML techniques used in intrusion detection. It offers solutions and concepts for further investigation into issues like imbalance network traffic data and incremental learning in intrusion detection.
- This paper conducts comparison experiments on several intrusion detection learning algorithms and gives data support for building the dominant algorithm model.
- Highlighting the main contributions, findings, and benefits of recent work done in the field of deep IDS and contrasting the evaluated metrics, simulators, feature selection techniques, and datasets of those studies.

2 INTRUSION DETECTION SYSTEMS

IDS is a hardware or software device that detects unusual network activity. IDS's major duties are network monitoring, breach detection, and reporting to the administrator [11-12]. When malicious behaviours are detected, advanced IDS can additionally take action, such

as banning traffic from the originating IP address [13]. There are two types of intrusion detection methods: anomaly detection and signature detection.

2.1.SIGNATURE BASED IDS

Organizations employ Signature-based IDS to defend against a variety of known threats, the signatures of which are stored in the database. An audited pattern was run through IDS against a list of known harmful bytes. IDS that utilize signatures can communicate the reason for an intrusion alert [14]. While signature-based IDS is able to quickly identify known assaults, it is ineffective against fresh threats whose patterns have not yet been discovered or updated in the database. This problem can be solved by routinely updating the patterns in the database. However, signature-based detection is not effective when the attacker uses sophisticated technologies, such as no operation (NOP) generators, payload encoders, and encrypted data channels, to mount the assault. With every alteration requiring a new signature, its effectiveness is drastically reduced.

2.2.ANOMALY BASED IDS

By monitoring anomaly-based IDS find network and computer breaches in the networks. After monitoring, it employs heuristics or rules to categorize the occurrences as either normal or anomalous and makes an effort to find abnormal operation [15]. Although designing the rule set of an anomaly detection approach can be difficult, it can detect unique assaults.

3 MACHINE LEARNING BASED INTRUSION DETECTION

Machine learning (ML), a branch of AI that studies numerous ways that may learn from data and then predict it, is one such technology. ML techniques often work using features that correspond to an object's characteristic. Data patterns can be found and learned using machine learning. Supervised learning and unsupervised learning are the two main subcategories of machine learning. Labelled data needs to have relevant information in order for supervised learning to function. Classification is the most common problem in supervised learning (and in IDS), yet manually tagging the data is costly and time-consuming. As a result, supervised learning's main challenge is a lack of enough annotated data. However, unsupervised learning is significantly simpler to implement because it can extract relevant feature information from unlabelled data. However, supervised learning techniques often outperform unsupervised learning approaches in terms of detection. The common machine learning techniques employed in IDSs are shown in Figure 1.

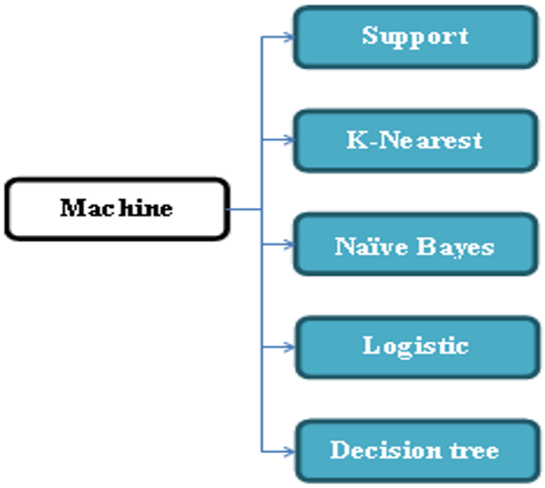

Fig.1. ML méthodes use in Intrusion détection system

3.1SUPPORT VECTOR MACHINE (SVM)

It is a supervised model used for classifying, regressing, and identifying outliers.Based on the hyperplane, the data are linearly separated. The data is transformed into feature space by SVM, which then classifies it using a hyperplane with the greatest distance between instances of each class. It is a binary classifier with multi-class classification capabilities. SVM is best suited for use with nonlinear data.

On the basis of sampling, Kabir et al.[16] suggested the feasible allocation based most tiny square SVM (OA-LS-SVM). Both static and incremental data can be handled using this method. The KDD 99 dataset is used to investigate and validate the suggested method. In terms of performance and accuracy, the suggested strategy yields a reasonable outcome.

Based on SVM ensemble with feature augmentation, Gu et al [17] suggest a method for efficient intrusion detection. To get new and higher-quality altered training data, the logarithm marginal density ratios transformation is specifically applied to the original features. The SVM ensemble was then utilized to develop the intrusion detection model. Results of the experiments reveal that the suggested approach has significant modest advantages over other methods already in use.

Liu et al [18] presents an integrated SVM and feature-analysis-based web IDS. The features of typical Web assaults are examined using expert knowledge. The analysis of the HTTP protocol chooses the relevant data attributes. The reliable SVMmethod is used in classification learning, and parameter optimization is accomplished using the grid search technique. As a result, it is possible to improve the ability to identify Web attacks. Experiments have been performed to look at the detection capabilities of various kernel functions using the HTTP DATASET CSIC 2010 data set.

Gu and Lu [19] introduced an effective IDS built by embedding the features of SVM and NB.Feature transformation is carried out by the naïve Bayes approach to provide the quality data from the raw input data. Finally the SVM is classified the different class of intrusion from the transformed data.This model is evaluated on UNSW-NB15 dataset and provides an effective detection strategy with an accuracy of 93.75%.

Compared to unsupervised approaches, Ali Ghorbani&SeyedMostafaFakhrahmad [20] suggest a unique supervised sparse auto-encoder that seeks to extract more meaningful data for classification models. Utilizing the data sets from NSL-KDD, KDDCUP'99, and CICIDS'17, this model is evaluated with detection rate and response time. The detection

rate and test time experimental results are promising. Binary classification achieved accuracy ratings of 91.21 on CICIDS2017 and 90.11 on NSL-KDDTest+.

3.2. K-NEAREST NEIGHBOR

ANN is used to solve classification and regression;however it's great for handling classification. Due to its laziness, it simply stores all training data. This information is used to identify patterns between old and new data. On the basis of Euclidean distance, the test data is categorized into the kNN class.

A hybrid IDS was suggested by Saleh et al[21] to address the multi-class classification issue with triple-edged strategy because of its three major contributions, which comprised (i) NBFS for feature selection, (ii) OSVM for outlier rejection, and (iii) PKNN for input attack detection. The HIDS was compared to more modern methods using the datasets. It may be utilized for real-time anomaly detection and proved effective in quickly detecting threats.

The KNN approach and the Improved Tree Seed Algorithm (ITSA) proposed by VikramRajpoot&RuchiAgrawal [22] to enhance the identification of intrusion. KNN is used for classification in the ITSA process after the most useful aspect of the input data is gathered. This study evaluates the effectiveness of the model using a variety of UCI data and KDDCUP 99 data sets.

Wazirali[23] suggested IDS using fivefold cross-validation on semisupervised learning and k-nearest neighbour hyperparameter tweaking. The training set's k-nearest neighbours are first found for each unlabelled data point. The NSL-KDD dataset, which is used to assess the model's robustness.

NerellaSameera& M. Shashi [24] examine the viability of encoding categorical features in the context of IDS depending on the posterior likelihood of an attack conditioned on the feature. IDS is built using a KNN classifier on top of latent characteristics that take the shape of numbers. To predict one of the 40 distinct class labels that could apply to a test instance, the suggested approach is trained and evaluated using the NSL-KDD data set. Performance measurements include detection accuracy and FPR. According to the results, the suggested method has a 98.05% accuracy rate for intrusion detection and a 0.35% false alarm rate.

3.3. LOGISTIC REGRESSION (LR)

Based on independent values, LR makes an estimate for the discrete values between 0 or 1. When data are fitted to a logistic function, the outcome of the event is predicted. A threshold value of 0.5 is used, and numbers over it are treated as 1, while values below it are treated as 0.

Palmieri [25] presented a unique method for detecting network anomalies that was centred on the Internet traffic's nonlinear invariant properties. The total results demonstrated that the method accurately and precisely separates a variety of volumetric DoS attacks that include intricate traffic patterns.

Boya Du and Fei Deng [26] employed principal component analysis to take into account the redundant data, then used the principle components as new variables to create the logistic model. The ideal cutting value and accompanying accuracy can be found using the confusion matrix and ROC curve. Finally, the CIC-IDS2017 dataset is used for testing and evaluation.

To give the best accuracy for attack detection, a new framework for intrusion detection using ensemble ML approach has been presented by Nitesh Singh Bhati&ManjuKhari [27]. Voting ensemble models have been integrated using fundamental learning techniques. On

the KDDCUP99 dataset, experiments with the suggested model have been done in order to help the intrusion detection system discover attacks. According to empirical findings, detection accuracy has improved across all network traffic classes. This model's effectiveness is indicated by its Accuracy Score of 99.86%.

3.4. NAIVE BAYES (NB)

Based on the notion of attribute independence and conditional probability, this algorithm is simulated using the Bayes rule. The Naive Bayes classifier determines the conditional probabilities for several classifications for each sample. The sample is put into the class with the highest probability. The calculation for the conditional probability formula is represented in Formula (1)

$$P(A=a|B=x\_k)=\prod\_(i=1)^n P(A^((i))=a^((i)) |B=x\_k) \quad (1)$$

The Naive Bayes method yields the best result when the attribute independence hypothesis is met.

A hybrid layered IDS that made use of several ML techniques was proposed by Çavusoglu[28] depending on the type of attack. Training and testing were conducted using the NSL-KDD dataset. The dataset underwent transformation and normalization processes. The results demonstrated that the suggested method produced outstanding accuracy as well as low FPR for all attack types.

Through analysis and evaluation methods carried out on the NSL-KDD dataset, Tabash et al [29] proposed a hybrid deep learning model that increases detection rate, accuracy, and lowers false alarms. Preparing and processing the dataset before the processing stage, choosing the proper features, lowering dimensions, and using the discretization technique to increase intrusion detection performance are the most crucial phases in creating an effective model.

Sukhvinder Singh et al. [30] presented the IDS methodology to detect malicious intent in the Software defined network (SDN) using the PCA feature selection approach which is linearly stable. In order to distinguish between normal and abnormal nodes, the collected features will next be classified using a brand-new poly logarithmic function-based NB classification algorithm.

Meerja et al. [31] suggest using IDS to detect intrusions through network traffic data. Because the network traffic data is continuous in nature, the Gaussian NB classification approach is used in conjunction with the IDS to determine the intrusions.To assess the effectiveness of the suggested approach, Kyoto dataset is adopted in this study. The findings demonstrate that the suggested approach outperforms the current approaches in terms of intrusion detection accuracy, intrusion detection rate, and FAR values.

3.5. ML TECHNIQUE CHALLENGES AND SOLUTIONS

From the aforementioned research, it can be inferred that many different forms of assaults have been detected using ML techniques. It enables the network administrator to respond to threats by taking appropriate countermeasures. However, the majorities of standard ML techniques are shallow learning (SL) techniques and frequently concentrate on feature selection. Traditional detection methods have a finite capacity for learning, and learning effectiveness further declines as network complexity increases. They can't successfully address the actual network application problem since they only represent a portion of the information. The multi-classification process will result in decreasing accuracy since data sets are expanding dynamically.

Decision trees are prone to over fitting and overlook the issues brought on by inter-data correlation, while logistic regression is simple to under fit and has low accuracy. Finding a good kernel function that can handle missing data can be difficult because SVM is ineffective when working with huge samples.

DL approaches, an advanced subset of ML, are attracting interest across many disciplines as a solution to these restrictions. Due to its many advantages over ML approaches, including automatic feature learning, flexible adaptability to unique challenges that make it possible to work with massive data, etc., it has drawn the attention of researchers. It's enhanced superior layer feature learning capabilities.

4. Deep learning based IDS

The review of intrusion detection approaches based on DL techniques is presented in this section. These techniques have benefited deep learning algorithms. Figure 4 shows how the deep learning-based IDS methods are categorized. DL approaches are often used in the feature extraction step, the classification step, or both of the analysed intrusion detection systems.

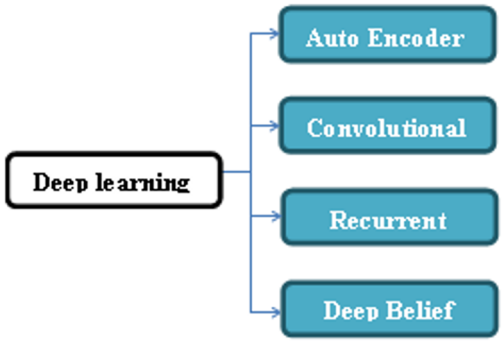

Fig. 2. DL methods used in Intrusion detection system

4.1. AUTO ENCODER

Song et al. [32] developed and assessed a stacked autoencoder model using several model setups. The latent size and model capacity had an effect on the NIDS performance, according to empirical results on applied intrusion data all collected from traditional and IoT networks. Our simple stacked autoencoder models generated the best F1-score of 0.895 using the NSL-KDD dataset.

The recurrent non-symmetric deep autoencoder (RNDAE) introduced by M. Srikanthyadav and R. Kalpana [33] for learning unsupervised features is described. Additionally demonstrated is a fresh deep learning classification model built on LightGBM RNDAEs. Using TensorFlow, the NSL-KDD, CICIDS 2017, and CSECICIDS 2018 datasets were used to assess our suggested classifier. The newest generation of network intrusion detection systems (NIDS) may adopt our concept if it stands up.

In order to strengthen the data's resilience after dimensionality reduction and to reduce the dimensionality of the nonlinear network data, Deng et al. [34] develop a denoising autoencoder network and a sparse autoencoder. The BP neural network is strengthened by the improved GA (IGA), resulting in the IGA-BP network. Finally, intrusion detection is performed via the IGA-BP network. In network infiltration problems, this approach is meant to address data dimension duplication and BP network local area minimization.

To categories IDS attacks, Kunang[35]presents automatic feature extraction using a basic autoencoder and SVM. In order to determine how much this feature extraction feature can increase accuracy, various functions activation and loss are applied. The efficiency of the detection techniques is then assessed using the 99 NSL-KDD datasets from the KDD Cup. The activating activities hyperparameter for the autoencoder In comparison to the other functions in the suggested model, ReLU activation and loss function cross-entropy offer the best accuracy value.

4.2. CONVOLUTIONAL NEURAL NETWORK

To simultaneously extract features from many classes of the original flow, Zhang et al. [36] suggested an enhanced feature extraction method. The suggested approach speeds up network convergence while simultaneously lowering the quantity of unnecessary elements for network learning. To address the real-time needs of network intrusion detection in the present big data computing, author also developed four enhanced variants of the PCCN network topology. These networks have nearly identical detection performance as the PCCN but significantly faster data detection.

A brand-new voting-based DL architecture, known as VNN, is suggested by Jun Li and Mohammad HashemHaghighat [37] to benefit from all different types of deep learning architectures. When many models produced by distinct deep learning architectures and diverse parts of the data are taken into account, VNN has the capacity to integrate the top models to generate outcomes that are more accurate and reliable.Security experts can detect more complex threats with the help of VNN.Experimental results with well-known and regularly used datasets in the computer network field, showed that False alarms dropped up to 75% compared to the original DL models, demonstrating the voting process's great effectiveness in enhancing system performance.

A hybrid intrusion detection system model was developed by AsmaaHalbouni et al [38] by combining the spatial feature extraction capabilities of a convolutional neural network with the temporal feature extraction capabilities of a LSTM network. The model's performance was improved with the addition of layers for batch normalization and dropout. The confusion matrix, which contains various evaluation factors, defines the system's performance. Experimental results demonstrated the effectiveness of the proposed model with a high detection rate, good accuracy, and a comparatively low FAR.

In order to effectively separate and identify network activity data and ensure the security of the Industrial Internet of Things (IIoT), Du et al. [39] provide a network intrusion detection classification model (NIDS-CNNLSTM) utilizing a deep learning technique. With time series data, NIDS-CNNLSTM combines the potent learning capabilities of LSTM neural networks, learns and categorizes the features selected by the CNN, and assesses the applicability using scenarios for binary and multi-classification. The traditional datasets NSL_KDD, and UNSW_NB15 are used for evaluation.

For IoT networks, ImtiazUllah and Qusay H. Mahmoud [40] design novel anomaly-based IDS. A multiclass classification model is initially developed using a CNN model. The proposed model is then put into practice utilizing 1D, 2D, and 3D convolutional neural networks. Utilizing intrusion detection datasets, the suggested CNN model is validated. To accomplish binary and multiclass classification, a CNN multiclass pre-trained model leverages transfer learning.

4.3. RNN

Hu et al [41] suggests a brand-new approach to intrusion detection that is based on the adaptive synthetic sampling (ADASYN) approach and an enhanced CNN. The ADASYN

technique is initially used by the author to balance the sample distribution, which prevents the predicted outcome from being sensitive to large samples and disregarding little samples. Second, the split convolution module (SPCCNN), that enhances the feature variety and reduce the negative implications of redundant interchannel data regarding training models, is the foundation of the improved CNN. Then, for tasks involving intrusion detection, an AS-CNN model combined with ADASYN and SPC-CNN is used. Finally, for AS-CNN testing, the default NSL-KDD dataset is used.The experiment reveals that, in comparison to the standard CNN and RNN models, the detection rate of prediction is 4.60 percent and 2.7% higher, respectively.

Yu et al [42] suggests a brand-new, adaptable, and reliable NIDS that uses a multi-classifier and a recurrent neural network (RNN) to create a detection model in real time. The suggested system intelligently and adaptively modifies the created model using the system characteristics that can be utilised as security parameters to block real-time obfuscation attacks from the attacker. According to the findings of the experiments, the suggested system identifies network attacks with high accuracy and real-time model upgrades while demonstrating robustness under an attack.

In order to strike a balance among dimensionality reduction and feature retention in unbalanced network data, Wu et al. [43] developed a Reliable Transformer-based IDS (RTIDS). The suggested method uses a modified stacked encoder-decoder to learn low-dimensional feature representations from high-dimensional raw input. To link sequential information between features, the positional embedding technique is used. A self-attention technique is also employed to facilitate categorizing various sorts of network traffic. The success of the proposed RTIDS is demonstrated thorough validation on two open access real network traffic datasets, CICIDS2017 and CIC-DDoS2019, with F1-Scores of 99.17% and 98.48%, respectively.

A strong defence against such unavoidable attacks is provided by FarisAlasmary [44]. The two components of the suggested approach are a server detector and an IoT node detector. The IoT node detector is a simple classifier that keeps track of exit traffic. The IoT node will employ the server detector, a more precise classifier, if it suspects that it is a part of a DDoS attack. This work suggests ShieldRNN, a unique training and prediction strategy for RNN/LSTM models, to create an accurate server detector. On the CIC-IDS2017 dataset, author compared proposed ShieldRNN with other traditional ML models and demonstrate its superior performance.

The gradient-clipping problem is resolved by the donkolet al [45] suggested solution using enhanced LSTM classification and probable point particle swarm optimization (LPPSO). The NSL-KDD dataset (KDD TEST PLUS and KDD TEST21) was used for validation and testing to assess the suggested technique. The particle swarm optimization, an improved technique, was used to choose several effective characteristics. The chosen characteristics are employed for efficient classification using an improved LSTM framework, which is used to distinguish attack data from regular data. The UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018, and BOT _DATASET datasets have all been used to apply the proposed approach in order to conduct additional verification.

4.4. DEEP BELIEF NETWORK

Wei [46] introduceda novel joint optimization method that enhances the structure of DBN's network. First, PSO is developed based on the learning factor and adaptive inertia weight. Then PSO is optimized to discover the first optimization solution using the fish swarm behaviour of cluster. The genetic operators with self-adjusting feature are then used to enhance the PSO in order to obtain the original optimization solution. The network

topology of the ID classification model is then created using the global optimization solution created by the aforementioned joint optimization method.

Wu et al. [47] introduced IDS by fusing feature-weighted SVM (WSVM) and deep belief networks (DBN). To improve the IDBN's training performance, that learn deep features from input data in order to reduce dimensionality, an adaptive learning rate technique is first employed. The SVM is then improved using the particle swarm optimization approach, and the resulting WSVM may eliminate weakly connected and duplicated features across all characteristics retrieved by IDBN after determining the optimum Gaussian kernel parameters and deep feature weights. The IDBN-WSVM model was validated using the NSL-KDD dataset. The efficacy of the model was specifically examined and contrasted against a model made up of a non-weighted SVM and other ML techniques. In both binary and multi class classification, the suggested approach obtains highest detection accuracies of 85.73 percent and 82.3 percent, respectively.

Kunal Singh and K. James Mathai [48] compared the performance of IDS using the DBN and SPELM approach. Prior research applied the SPELM in various field like image processing (face recognition), intrusion identification model and pedestrian detection.The performance of DBN on intrusion dataset is evaluated and compared with SPELM algorithm. The NSL-KDD dataset contains four lakhs of data records, of which 40% were used for testing and 60% for training when determining the effectiveness of both algorithms.

In a network of interconnected devices, OthmaneBelarbi et al. [49] develop and assess the effectiveness of Deep Belief Networks (DBNs) in detecting cyber-attacks. The CICIDS2017 dataset was utilized to train our proposed DBN technique and assess its effectiveness. Numerous class balancing strategies were used and assessed.

NagarajBalakrishnan et al [50] developed an intelligent approach or technique to guard against a security attack by improving Deep Belief Network. This highly developed intrusion detection system looks at hostile activity that is present within the network and seeks to get access. This paper investigates the embedding of the Deep Learning approach. The DBN augmentation of the security network is compared to typical DGAs and IDS algorithms, and the results are reviewed.

5. Discussion

According to the findings of the previous section, the majority of the schemes employed datasets based on KDDCup, which are outdated and unable to accurately represent contemporary security threats and assaults. Due to the shortcomings of the available datasets, additional datasets in the IDS context and across other domains should be produced in order to thoroughly verify the recently suggested IDS techniques.

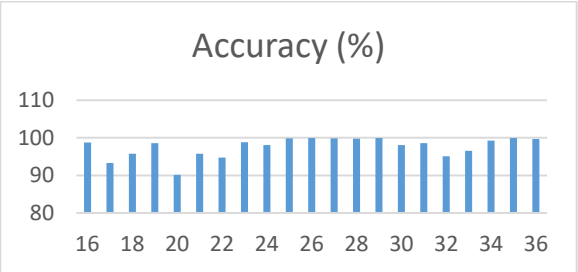

Fig. 3. Detection Accuracy achieved on each article

High-level languages like Python are easier to learn, easier to read, and more portable. Because it is a low-level language, MATLAB struggles with some algorithms, such those in bioinformatics. The matrix function is accessible in MATLAB, and Python users can use NumPy to access the library and obtain comparable results. In literature some research utilized MATLAB for simulation and recent studies applied python for implementation. With the ease in algorithm implementation and accurate result Python is suggested by several researches.

The proposed methods can be categorized as either dealing with unencrypted traffic or dealing with encrypted traffic depending on the kind of traffic that the examined IDS schemes can handle. However, there aren't many methods available for detecting eavesdropping on encrypted trafzvdfic. Therefore, additional research on encrypted traffic seems necessary for various domains. Deep learning approaches often require a lot of processing, and as they apply more neurons and layers, their training latency and computation complexity increase as well. Furthermore, methods like cross-validation, which are employed to lessen the over-fitting issue in a deep IDS scheme when a large dataset is used, can result in additional training costs. The literature suggests a number of strategies to address this problem. The performance of existing methods are analysed and showed in figure 3.

To accelerate the learning rate of deep approaches, alternative ways to improve deep network training performance should be investigated. Distributed deep learning is one of the intriguing options to cope with the training pace of the DL methods. Model parallelism and data parallelism strategies are provided for training the deep model in a distributed environment. Model parallelism demands that a single model process all of the data and that each node take part in estimating the parameters of the model. Another noteworthy strategy for lowering deep learning network training time is transfer learning, which can be done with pre-trained model.This technology can be investigated further to improve the intrusion detection mechanism in future IDS solutions.

In the literature most of the studies concentrated on the intrusion detection mechanism. A end to end security system is enable through detection and prevention techniques. The intrusion prevention system (IPS) is a significant process in developing a complete security system. IPS refers to the punitive action the system takes in the event of an incursion. False positives in IPS present a problem because they can also block legitimate users.The intrusion prevention can be developed using cryptography, block chain, ML and DL approaches [51].

6. Conclusion

This article provides a comprehensive overview and classification of IDS that have aided deep neural networks in dealing with assaults and hostile behaviours. To that end, it first categorizes deep IDS schemes based on the deep learning techniques they integrate, and then explains how each scheme attempts to employ DL approaches to recognize distinct sorts of intrusions. Furthermore, the shallow learning methods used in conjunction with deep learning approaches are evaluated in the analysed deep IDS schemes. Furthermore, to provide a thorough understanding of the investigated IDS frameworks, the key contributions, advantages, and limits of each approach are outlined in each area. Furthermore, the evaluation metrics, simulators, and datasets used in each category are contrasted. Finally, it is possible to conclude that deep learning is an intriguing technology that presents numerous opportunities as well as obstacles in the context of intrusion detection.

References

1. U. S. Musa, M. Chhabra, A. Ali, and M. Kaur, ‘‘Intrusion detection system using machine learning techniques: A review,’’ in Proc. Int. Conf. Smart Electron. Commun. (ICOSEC), Sep. (2020), pp. 149–155.
2. Ring, Markus, Sarah Wunderlich, DenizScheuring, Dieter Landes, and Andreas Hotho. "A survey of network-based intrusion detection data sets." Computers & Security 86 (2019): 147-167.
3. Z.H. Wu, “Information Security Technology and Practice”, (2019)
4. Xin, Yang, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, MingchengGao, HaixiaHou, and Chunhua Wang. "Machine learning and deep learning methods for cybersecurity." Ieee access 6 (2018): 35365-35381.
5. Gumusbas, Dilara, and TulayYildirim. "AI for Cybersecurity: ML-Based Techniques for Intrusion Detection Systems." Advances in Machine Learning/Deep Learning-based Technologies: Selected Papers in Honour of Professor Nikolaos G. Bourbakis–Vol. 2 (2022): 117-140.
6. Handa, Anand, Ashu Sharma, and Sandeep K. Shukla. "Machine learning in cybersecurity: A review." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 9, no. 4 (2019): e1306.
7. Aleesa, B. Zaidan, A. Zaidan, and N. M. Sahar, ‘‘Review of intrusion detection systems based on deep learning techniques: Coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions,’’ Neural Comput. Appl., vol. 32, pp. 1–32, Jul. 2020.
8. S. Osken, E. N. Yildirim, G. Karatas, and L. Cuhaci, ‘‘Intrusion detection systems with deep learning: A systematic mapping study,’’ in Proc. Sci. Meeting Elect.-Electron. Biomed. Eng. Comput. Sci. (EBBT), Apr. 2019, pp. 1–4
9. Aldweesh, A. Derhab, and A. Z. Emam, ‘‘Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,’’ Knowl.-Based Syst., vol. 189, Feb. 2020, Art. no. 105124
10. R. Vinayakumar, K. P. Soman, and P. Poornachandran, ‘‘A comparative analysis of deep learning approaches for network intrusion detection systems (N-IDSs): Deep learning for N-IDSs,’’ Int. J. Digit. Crime Forensics, vol. 11, no. 3, pp. 65–89, Jul. 2019.
11. Vinayakumar R, Alazab M, Soman K, Poornachandran P, Al-Nemrat A, Venkatraman S (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7:41525–41550.
12. Almomani A, Alauthman M, Albalas F, Dorgham O, Obeidat A (2020) An online intrusion detection system to cloud computing based on neucube algorithms. In: Cognitive analytics: concepts, methodologies, tools, and applications. IGI Global, pp 1042–1059.
13. Chevalier R, Plaquin D, Villatel M, Hiet G (2020) Intrusion detection systems. US Patent App. 16/486,331.
14. Jacob NM, Wanjala MY (2018) A review of intrusion detection systems. Glob J ComputSciTechnol 5:66
15. Farzaneh B, Montazeri MA, Jamali S (2019) An anomaly-based ids for detecting attacks in rpl-based internet of things. In: 2019 5th International conference on web research (ICWR). IEEE, pp 61– 66.

16. Kabir E, Hu J, Wang H, Zhuo G (2018) A novel statistical technique for intrusion detection systems. FutGenerComputSyst 79:303–318.
17. Gu, Jie, Lihong Wang, Huiwen Wang, and Shanshan Wang. "A novel approach to intrusion detection using SVM ensemble with feature augmentation." Computers & Security 86 (2019): 53-62.
18. Liu, Chao, Jing Yang, and Jinqiu Wu. "Web intrusion detection system combined with feature analysis and SVM optimization." EURASIP Journal on Wireless Communications and Networking 2020 (2020): 1-9.
19. Gu J, Lu S (2021) An effective intrusion detection approach using SVM with Naïve Bayes feature embedding. ComputSecur 103:102158.
20. Ghorbani, Ali, and SeyedMostafaFakhrahmad. "A deep learning approach to network intrusion detection using a proposed supervised sparse auto-encoder and svm." Iranian Journal of Science and Technology, Transactions of Electrical Engineering 46, no. 3 (2022): 829-846.
21. Saleh AI, Talaat FM, Labib LM (2019) A hybrid intrusion detection system (hids) based on prioritized k-nearest neighbors and optimized svm classifiers. ArtifIntell Rev 51(3):403–443
22. Rajpoot, V., Agrawal, R. (2022). ITSA-KNN: Feature Selection Model Based on Improved Tree-Seed Algorithm and K-Nearest Neighbor for Network Intrusion Detection. In: Tiwari, S., Trivedi, M.C., Kolhe, M.L., Mishra, K., Singh, B.K. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 318.
23. Wazirali, R. An Improved Intrusion Detection System Based on KNN Hyperparameter Tuning and Cross-Validation. Arab J SciEng 45, 10859–10873 (2020).
24. Sameera, N., Shashi, M. (2020). Encoding Approach for Intrusion Detection Using PCA and KNN Classifier. In: Raju, K., Govardhan, A., Rani, B., Sridevi, R., Murty, M. (eds) Proceedings of the Third International Conference on Computational Intelligence and Informatics . Advances in Intelligent Systems and Computing, vol 1090.
25. Palmieri F (2019) Network anomaly detection based on logistic regression of nonlinear chaotic invariants. J NetwComputAppl 148:102460
26. B. Du and F. Deng, "The method of network intrusion detection based on descriptive statistics model and Logistic model," 2022 International Conference on Machine Learning and Knowledge Engineering (MLKE), Guilin, China, 2022, pp. 160-163
27. Bhati, N.S., Khari, M. (2022). An Ensemble Model for Network Intrusion Detection Using AdaBoost, Random Forest and Logistic Regression. In: Unhelker, B., Pandey, H.M., Raj, G. (eds) Applications of Artificial Intelligence and Machine Learning. Lecture Notes in Electrical Engineering, vol 925.
28. Çavuşoğlu, Ü. A new hybrid approach for intrusion detection using machine learning methods. ApplIntell 49, 2735–2761 (2019
29. Tabash, M., Abd Allah, M. and Tawfik, B., 2020. Intrusion detection model using naive bayes and deep learning technique. Int. Arab J. Inf. Technol., 17(2), pp.215-224.
30. Singh, S., 2022. Poly Logarithmic Naive Bayes Intrusion Detection System Using Linear Stable PCA Feature Extraction. Wireless Personal Communications, 125(4), pp.3117-3132.
31. A.J., Ashu, A., RajaniKanth, A. (2021). Gaussian Naïve Bayes Based Intrusion Detection System. In: Abraham, A., Jabbar, M., Tiwari, S., Jesus, I. (eds) Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition

(SoCPaR 2019). SoCPaR 2019. Advances in Intelligent Systems and Computing, vol 1182.

32. Song, Y., Hyun, S. and Cheong, Y.G., 2021. Analysis of autoencoders for network intrusion detection. Sensors, 21(13), p.4294.
33. Kalpana, R. "Recurrent nonsymmetric deep auto encoder approach for network intrusion detection system." Measurement: Sensors 24 (2022): 100527.
34. Deng, H. and Yang, T., 2021. Network intrusion detection based on sparse autoencoder and IGA-BP network. Wireless Communications and Mobile Computing, 2021, pp.1-11.
35. Y. N. Kunang, S. Nurmaini, D. Stiawan, A. Zarkasi, Firdaus and Jasmir, "Automatic Features Extraction Using Autoencoder in Intrusion Detection System," 2018 International Conference on Electrical Engineering and Computer Science (ICECOS), Pangkal, Indonesia, 2018, pp. 219-224.
36. Y. Zhang, X. Chen, D. Guo, M. Song, Y. Teng and X. Wang, "PCCN: Parallel Cross Convolutional Neural Network for Abnormal Network Traffic Flows Detection in Multi-Class Imbalanced Network Traffic Flows," in IEEE Access, vol. 7, pp. 119904-119916, 2019.
37. M. H. Haghighat and J. Li, "Intrusion detection system using voting-based neural network," in Tsinghua Science and Technology, vol. 26, no. 4, pp. 484-495, Aug. 2021
38. A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022.
39. J. Du, K. Yang, Y. Hu and L. Jiang, "NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning," in IEEE Access, vol. 11, pp. 24808-24821, 2023,
40. I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021
41. Z. Hu, L. Wang, L. Qi, Y. Li and W. Yang, "A Novel Wireless Network Intrusion Detection Method Based on Adaptive Synthetic Sampling and an Improved Convolutional Neural Network," in IEEE Access, vol. 8, pp. 195741-195751, 2020
42. K. Yu, K. Nguyen and Y. Park, "Flexible and Robust Real-Time Intrusion Detection Systems to Network Dynamics," in IEEE Access, vol. 10, pp. 98959-98969, 2022
43. Z. Wu, H. Zhang, P. Wang and Z. Sun, "RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System," in IEEE Access, vol. 10, pp. 64375-64387, 2022.
44. F. Alasmary, S. Alraddadi, S. Al-Ahmadi and J. Al-Muhtadi, "ShieldRNN: A Distributed Flow-Based DDoS Detection Solution for IoT Using Sequence Majority Voting," in IEEE Access, vol. 10, pp. 88263-88275, 2022.
45. A. A. E. -B. Donkol, A. G. Hafez, A. I. Hussein and M. M. Mabrook, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks," in IEEE Access, vol. 11, pp. 9469-9482, 2023
46. P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li and D. Liu, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," in IEEE Access, vol. 7, pp. 87593-87605, 2019.

47. Y. Wu, W. W. Lee, Z. Xu and M. Ni, "Large-Scale and Robust Intrusion Detection Model Combining Improved Deep Belief Network With Feature-Weighted SVM," in IEEE Access, vol. 8, pp. 98600-98611, 2020.
48. K. singh and K. J. Mathai, "Performance Comparison of Intrusion Detection System Between Deep Belief Network (DBN)Algorithm and State Preserving Extreme Learning Machine (SPELM) Algorithm," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019,
49. Balakrishnan, Nagaraj, ArunkumarRajendran, DaniloPelusi, and VijayakumarPonnusamy. "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things." Internet of things 14 (2021): 100112.
50. Belarbi, O., Khan, A., Carnelli, P., Spyridopoulos, T. (2022). An Intrusion Detection System Based on Deep Belief Networks. In: Su, C., Sakurai, K., Liu, F. (eds) Science of Cyber Security. SciSec 2022. Lecture Notes in Computer Science, vol 13580.