Internet of Things: A Review on Machine Learning-based Intrusion Detection System

Priyanka Gupta
Department of computer science and engineering
Maulana Azad National Institute of Technology
Bhopal, India
priyankagupta2401@gmail.com

Lokesh Yadav
Department of computer science and engineering
Maulana Azad National Institute of Technology
Bhopal, India
lokeshcsenita@gmail.com

Deepak Singh Tomar
Department of computer science and engineering
Maulana Azad National Institute of Technology
Bhopal, India
deepaktomarmanit@gmail.com

***Abstract*—The Internet of Things (IoT) connects billions of interconnected devices that can exchange information with each other with minimal user intervention. The goal of IoT to become accessible to anyone, anytime, and anywhere. IoT has engaged in multiple fields, including education, healthcare, businesses, and smart home. Security and privacy issues have been significant obstacles to the widespread adoption of IoT. IoT devices cannot be entirely secure from threats; detecting attacks in real-time is essential for securing devices. In the real-time communication domain and especially in IoT, security and protection are the major issues. The resource-constrained nature of IoT devices makes traditional security techniques difficult. In this paper, the research work carried out in IoT Intrusion Detection System is presented. The Machine learning methods are explored to provide an effective security solution for IoT Intrusion Detection systems. Then discussed the advantages and disadvantages of the selected methodology. Further, the datasets used in IoT security are also discussed. Finally, the examination of the open issues and directions for future trends are also provided.**

Keywords—***Machine Learning, Deep Learning, Intrusion Detection, Internet of Things, Network Security.***

I. INTRODUCTION

With the exponential growth of IoT applications, approximately 20.4 billion devices online in 2020, and the number expected to increase by 75 billion by the end of 2025. Different sensors embedded in IoT systems allow them to acquire and process data remotely in real-time. The data obtained from the sensors help them to make intelligent decision-making systems and handle IoT environments effectively [3]. Users can control their devices from anywhere, anytime, which leads to the vulnerability of multiple threats. Security threats that are harmful to Users are (1) Unauthorized access to personal information and misuse of it; (2) endorsing attacks on other systems; and (3) growing security risks [1]. IDSs are required to keep the IoT networks protected and available to detect intruders. IoT devices have limited computation and power resources (bandwidth, battery, memory, and computation), so a complex Intrusion Detection System (IDS) cannot be implemented.

It is becoming imperative to improve research in this field of detecting intrusion in computer networks. Denial of service (DoS) is an acute devastating attack that blocks legitimate customers from accessing the resources they have paid [4], which breaches the terms of the Service Level Agreement (SLA), which results in enormous monetary damages for businesses and organizations. Besides, DoS also impacts small networks, such as smart houses, intelligent healthcare systems, intelligent agriculture systems, etc. [2]. DoS attacks that affect vital, intelligent applications such as healthcare can also lead to human death, as regular services are delayed. IoT gadgets (e.g., air conditioners, smart refrigerators, and smart televisions) are easily targeted by attackers who manipulate their flaws to carry out DoS attacks [4]. Thus, one of the essential issues for researchers today is to protect these devices. Intrusion detection is investigated worldwide to resolve this issue. Based on the detection, IDS are divided into signature-based, Specification-based, and anomaly-based.

In signature-based methods, when the device or network activity analyze an attack based on the signature stored in the internal IDS databases, IDSs attack detected. A warning will be activated if some device or network operation correlates with stored patterns/signatures. In identifying identified threats, this method is reliable and very successful, and its mechanism is simple to understand. However, to classify new attacks and discrepancy of existing threats, this strategy is unsuccessful since a corresponding signature is still unknown for such attacks [3, 4].

Anomaly-based IDS measures a system's operations to a standard behavior profile and produces an alarm if a normal behavior variance crosses a threshold. However, it seems that it does not adhere to a normal pattern to classify an intrusion, and understanding the full spectrum of normal behavior is not a straightforward process. This method is useful in identifying new threats. Typically, therefore this approach has false-positive rates very high [3-5].

The specification-based method is a collection of rules and thresholds that describe network modules such as routing tables, protocol, and nodes as expected behavior. Intrusions are observed by specification-based methods as network activity deviates from specifications definitions. Therefore, the same goal of anomaly detection is given to specification-based detection: to recognize anomalies from behavior normal. However, one crucial distinction between these methods is in the specification-based technique; each specification's rules should be specified by a human expert manually [1-5]. Compared with anomaly-based identification, manually defined parameters typically have lower false-positive rates. Specification-based detection systems, however, do not need a training process because they can start operating directly after setting up the specification [4].

In a popular application for detecting network attacks like IoT networks, ML/DL-related techniques have recently acquired a reputation. So, in IoT environments, ML/DL-based approaches can monitor benign and anomalous activity.

Network traffic was collected and investigated to understand regular patterns used in IoT devices. To detect abnormal behavior, any divergence from these normal trained behaviors can be used to forecast zero-day or new attacks by ML/DL-based approaches that have been studied. This paper focuses on various strategies to detect anomaly-based intrusion detection by ML/DL techniques.

The remaining study is structured as follows. Section 2. Discussion about the research work that uses the traditional and new ML/DLtechnique to IoT networks and discusses relevant literature-related contributions to IoT IDS methods. Section 3. presents some datasets that are widely used. Section 4. illustrates the discussion on an open challenge and future challenge to IoT security. Finally, Section 5 states conclusions for research in IoT security.

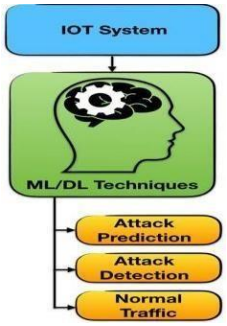

Fig 1. Role of ML/DL based IDS for IoT System

A. *Motivation*

Recently, a lot of work has been done related to IoT devices and gained attention that makes human activities easier, also use in the academic field and even within the industry. IoT is a possible option for improving people's quality of life (e.g., a smartwatch that tracks health through its sensors, smart home), and a variety of innovations have become desired with the drop in sensor costs, due to the remote storage facilities, and significant data IoT devices become popular. Simple access to such services explicitly reinforces IoT by integrating devices with various resources to a network, thereby leading to new applications [3]. A price has appeared less, so there is a need for security. Besides, there is doubt about the degree of trust in the data collected from IoT products, and how or when this knowledge can be used is one of the reasons for research [5].

Different surveys have presented numerous techniques for modeling IDS for IoT applications; however, several surveys have not comprehensively addressed ML / DL methods implementation to detect IoT intrusion. The main objective of this analysis is to compile recent works and discuss various methodologies.

II. RELATED WORK

This module has introduced a literature survey that uses modern and conventional algorithms focused on ML/DL algorithms to cope with IoT environments' security problems. The so-called "Systematic Review Literature" (SRL) was followed in the context of collecting the work considered in this survey. Methods can be defined, analyzed, and interpreted meaningfully using SRL methodology.

The use of ML to promote defense and identification in IoT systems has become increasingly necessary in recent years to tackle the previously mentioned challenges. In terms of security problems in IoT-based systems, overlooked too many works that used the ML and DL algorithm. In the last few years, the DL algorithm has also gained tremendous interest. DL algorithm is relevant to intrusion detection in networks.

A. ML Techniques for IDS

In this section, a summary of the various ML approaches used in IoT-based IDS environments is discussed. Table 1 presents a concise overview of the ML approaches, their benefits, and drawbacks. Fig 2 describes the ML methodologies used for detecting IDSs in an IoT environment.

K-Nearest Neighbour (KNN) is a nonparametric approach. The Euclidean distance is used as the distance metric by the KNN classifier. KNN method is used to detect new sample data into various categories based on the number of closest maximum neighbours from each class. A significant step in deciding the optimum value of k for a taken dataset is to evaluate various k values at the cross-validation time. Even though the KNN classifier is a basic algorithm for classification and efficient for the large training dataset, obtaining the feasible value of k may be a difficult and time is taken process. In [6] author suggested a model for the identification of R2L and U2R threats.

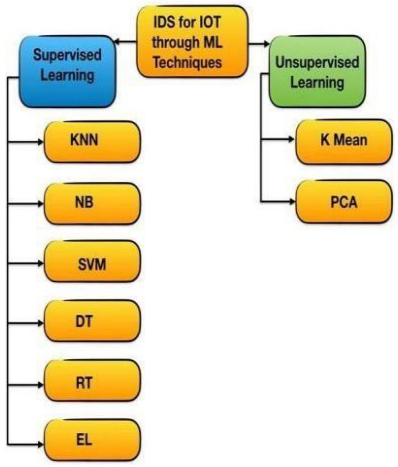

Fig.2.ML Methodologies for IoT based IDSs

The algorithm decreased the dimensionality of the features to improve reliability by using two feature reduction levels and then added a two-tier classification model using NB and KNN classifiers; this model showed promising results for detecting attacks.

Naïve Bayes (NB) classifier uses Bayes' theorem to estimate an occurrence based on prior observations of related events. This can be used in ML scenarios to distinguish normal and unusual behaviors based on previous findings in the supervised learning model. NB estimates the later likelihood, and a labeling determination to mark unlabeled traffic as normal or anomalous is taken based on that. An independent collection of observed traffic features such as status flags, protocol, and latency are used To estimate the possibility of traffic being regular [10]. Different IDS have used the NB method to classify abnormal traffic as it is quick and fast to incorporate an algorithm. In [7] author suggests that DoS threat identification is correlated with traffic information from the network. It needs relatively few training samples and can be categorized into both binary and multi-label classifications. NB classifiers are unable to capture valuable information from the associations and interactions between characteristics.

Interactions between characteristics can be critical for precise classification in complex samples. Inter-relation between characteristics can substantially help the method increase its ability to distinguish between classes.

Support Vector Machine (SVM) is another classifier method that operates on two or more classes' features through the formation of a hyperplane. SVMs are useful for use when classes with a broad set of features need to be categorized based on smaller data samples. SVM can create a hyperplane that delivers optimum margin. The strengths of SVMs are their flexibility and their ability to detect intrusions in real-time and change training patterns. However, it is essential to explore the output of SVM with large databases and datasets that are generated in multiple conditions and scenarios [8]. Another gain of using SVM is its lower memory/storage consumption. In separate research studies [9], the use of SVM in IDSs in an IoT method was tested, where SVM gives more precise results in comparison to other ML classification methods, including NB and RT. However, it remains a challenge to obtain the necessary classification using the ideal kernel function used in SVM to isolate the data sample, which is not linearly separable.

Decision Trees (DTs) collects sample characteristics from a dataset and arranges a tree based on feature value. Each of the features is classified by a tree node, and the branches from a node denote subsequent values. The tree's root node is known to be any function node that optimally splits the tree into two. Various metrics are used to define the origin node, which separates training datasets such as the Gini index and Information Gain optimally [10]. DTs have the ability to be used as classifiers in the field of intrusion detection. However, attention must be given to elements of more significant storage needs and computing complexity. An analysis reported in [10] in the IoT environment has used DT to classify DDoS attacks by evaluating network traffic to identify abnormal sources.

Random Forest (RF) is used to predict more precise and error-tolerant classification outcomes; an RF is constructed using multiple DTs. Randomly built DTs are trained on voting-based performance classification. Although DT can be viewed as RF, there are different algorithms for classification since RF creates a rule- subset using all member DTs, unlike DT, which constructs a rule through training to classify new data points. This result is a more stable and precise performance that tackles the overfitting and requires considerably fewer inputs, and does not need the feature selection process [12]. RF is ideal for intrusion detection in IoT networks, as suggested by several studies. Another research [13] has shown that RF in IoT networks is giving better results than KNN and SVM in DDoS classification because it needs fewer inputs. However, in particular, in real-time detection in which the necessary training dataset is large, the use of RF could be inefficient because RF requires the development of many DTs.

Ensemble Learning (EL) combines all the outputs of various simple classification methods to generate a combined output and enhance classification efficiency. To achieve a final answer, the EL goal to merge different or same multi-classifiers [11]. However, since EL contains multiple classifiers, the computation of an EL-based system is more than that of a single classifier-based system, leading to an increase in time complexity. For anomaly-based intrusion detection and malware detection [11-13], EL was used effectively. A previous study [13] shows that it is possible to reduce the time complexity of models to make it acceptable for devices with minimal hardware resources in IoT devices. Different experiments have tested the effectiveness of EL for intrusion detection.

K- Mean Clustering is an unsupervised algorithm focuses on the identification of k cluster in datasets. Each class of sample data is allocated to a specific cluster according to its characteristics. Data points are distributed on k clusters based on their behavior using the squared Euclidean distance. The recomputation of the centroids is then done by calculating the mean of the data points assigned to that cluster. The method proceeds iteratively until no improvements can be made to the clusters [14]. The specification of k and presumption are taken value is that the dataset will be spread uniformly on the k clusters serve as drawbacks for this algorithm. Recent research discussed in [14] indicates the use of a k-means clustering algorithm to detect anomalies by measuring the similarity of features.

Principle Component Analysis (PCA) is a feature selection or feature reduction technique used to convert a large dataset of features into a minimal set to retain much of the details in the dataset and is not an anomaly detection technique. After reduction, the identified feature can be used with specific other ML classifiers to identify anomalies on the IoT network [14-15].

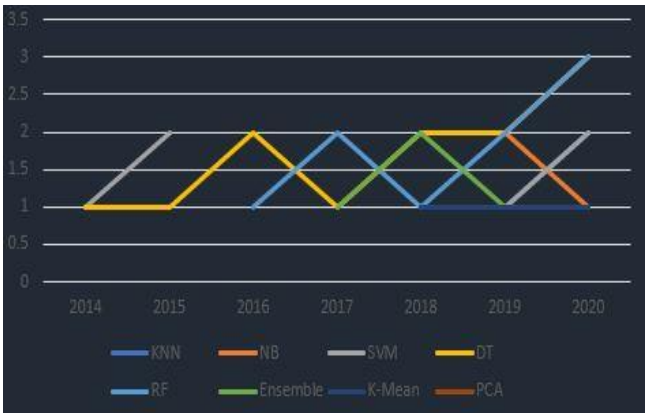

Fig.3. Machine Learning based IDS publication in IoT over years

Fig.3 shows statistical results on different ML algorithms-based publication in IoT IDS up to December 2020 which is still increasing.

B. DL Techniques for IDS

The implementation of the DL algorithm in IoT devices has recently been an essential focus of research [42]. It gives good performance in massive datasets is the most significant benefit of DL over conventional ML. Many IoT systems generate a vast volume of real-time data; hence, DL methods are sufficient for such systems [16, 17]. Various DL-based strategies used for constructing an IDS are described in this section. Table 2 shows a research study using different DL-based approaches to develop IDS. In the respective sub-sections below, details about research work are explained with the several DL methodology.

Convolutional Neural Network (CNN) is used to reduce the amount of sample data inputs needed for a traditional neural network using equal representation, sparse interaction, and parameter sharing [16]. CNN consists of a three-layer convolutional layer, pooling layer, and activation unit. For convoluting data inputs, the convolutionary layers use separate kernels [18].

Samples are reduced by the pooling layers, minimizing the sizes of successive layers through Max pooling and average pooling. CNN is applied for extracting highly effective and fast features from raw data, but CNN needs high computing capacity at the same time. Using CNN in resource-constrained IoT systems is therefore incredibly difficult for their security. In prior research published in [16- 18], malware detection and use in IoT environment protection were addressed.

Recurrent Neural Networks (RNNs) is also DL based discriminative algorithm that is ideally designed for a system where sequential processing of sample data is necessary. Unlike other neural networks, instead of forwarding propagation, its performance depends on backpropagation [19]. In the IDS design, long short-term memory (LSTM) network systems are used for RNN. The primary attribute of this is that information survives for later network use. This purpose makes them ideal for conducting temporal data analysis that varies over time. LSTM is also solved time-series sequence data related to anomaly detection. Various types of RNNs, including LSTM-based RNNs, were used by researchers in [20] intrusion detection in IoT networks. Although RNNs have shown encouraging results in forecasting time series data, it is still challenging to identify anomalous traffic using these predictions.

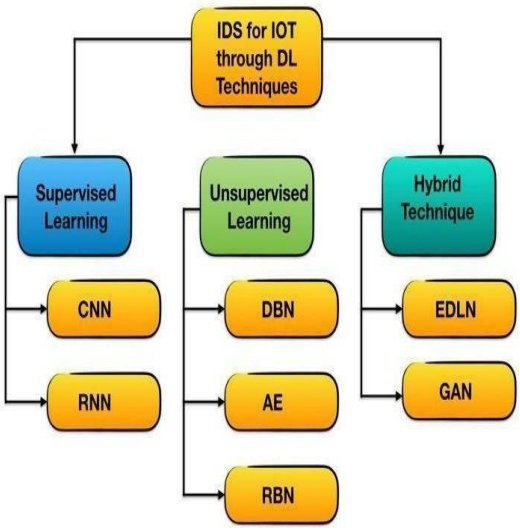

Fig 4. Taxonomy of DL techniques for IoT IDS

Deep Autoencoders is an unsupervised algorithm designed to replicate its input samples to its output through a function, and a code contains hidden layer descriptions used for input presentation [21]. In an Autoencoders (AE) neural network, the other function is known as the encoder function. It is defined for translating the information represented into code where reconstruction errors should be reduced during preparation [22]. Feature extraction from the datasets is one use case for AE. These suffer from the need for high computing capacity. It gives better accuracy than SVM and KNN for detecting network malware [22].

Restricted Boltzmann Machine (RBM) generates a generative, undirected model. In every layer of an RBM, there are no two nodes that have any relation with each other. The two kinds of layers that compose an RBM are visible and hidden layers. The predetermined input parameters are found in the visible layer, while multiple layers comprising the hidden layer are included in the possible unknown variables. Features derived from a dataset are then moved on to the next layer. A survey [23] shows that RBN is used to detect Intrusion detection in IoT networks. RBN requires high computing resources, so it is challenging to implement in IoT devices.

Deep Belief Network (DBN) is an unsupervised learning-based generative algorithm that can be formed by stacking two or more RBNs. In the pre-training process for each layer, initial features are extracted, then a fine-tuning step where the implementation of the softmax function layer is performed on top of the layer. It consists basically of two layers, namely the visible layer and the hidden layer. At the same time, the research in [24] addressed the detection of malicious attacks

using DBN and gave better results than most of the ML algorithms. The Generative Adversarial Network (GAN) uses generative and discriminatory models for training [17]. The generative model learns and generates data samples from the distribution of data, and the discriminative model estimates the probability that an input sample is generated from the training dataset rather than the generative model. The goal of training this model to increase the likelihood that the discriminative model misclassifies the sample. The discriminative output model lets the generative model boost the input samples produced for the previous iteration. The research published in [25] addressed the GAN algorithm's effectiveness to detect suspicious behavior in IoT systems with positive findings due to their potential to counter zero-day attacks by producing samples that imitate zero-day attacks, then enabling the discriminator to train various scenarios of attacks. The difficulty of using GAN, however, is that its preparation is challenging and creates unpredictable outcomes. Ensemble of DL Networks (EDLN) is a collection of DL algorithms that can perform better than algorithms applied independently.

It is possible to obtain EDLNs by combining generative, discriminatory, or hybrid ones. Further studies and analysis are necessary to use the EDLN to IoT security to determine the likelihood of enhancing the IoT system's efficiency and accuracy to resolve a challenge due to computation complexity [16-25].

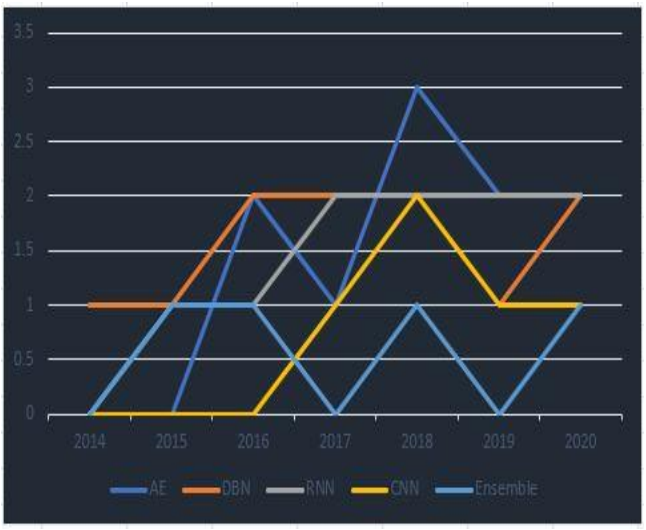

Fig.5. Deep Learning based IDS publication in IoT over years

Fig.5 shows statistical results on different DL algorithms-based publication in IoT IDS up to December 2020 which is still increasing.

Table.1 ML-BASED TECHNIQUE FOR IOT IDS

ML Methods	Attack Type	Advantages	Disadvantages
NB[7,10]	HTTP attacks (Shell attacks, Buffer overflow), Probe, DoS, R2L	• Fewer samples are required for training. • Classify both multi-label and binary classification. • For irrelevant features, it shows the robustness	• It fails when the features are interdependent, which affects its accuracy.
KNN[6]	U2R, R2L, Flooding attacks, DoS, DDoS	• Easy to use.	• Determining the best K value and finding missed nodes are challenging problems.
DT[10]	DDoS, U2R, R2L	• Simple and easy to use.	• It requires extensive storage and computationally complex • It is easy to use only if fewer DTs are constructed.
SVM[8,9]	Scan, DDoS (TCP, UDP flood), smurf, port sweep	• SVMs are incredibly versatile so that they can handle real-time tasks like anomaly-based intrusion detection and online learning. • SVMs are thought to be appropriate for data with a broad range of feature attributes. • SVMs consume fewer resources and storage.	• Achieving the desired classification using the optimum kernel function in SVM, which is used to separate data when it is not linearly separable, remains a problem. • SVM-based models are difficult to understand and analyze.
RF[12,13]	DoS, U2R, Probe, R2L	• It generates a more reliable and precise output that is less prone to overfitting. • It needs much fewer inputs and does not necessarily require the feature selection process.	• • Since RF produces several DTs, it can be inefficient to use in real-time applications that require a large dataset.
K-Mean[14]	DoS, Probe, U2R, R2L	• Labeled data are not required in k-Mean.	• It is less effective than supervised learning methods at predicting known threats.
PCA[14-15]	It combines with another classifier to detect Dos attack	• PCA is appropriate when the dataset contains a large number of variables since it reduces the number of features without compromising any details.	• Reduces the complicated amount of data. • It isn't a process for analyzing abnormalities. It must be associated with other machine learning approaches to construct a security model.

Table.2 DL BASED TECHNIQUE FOR IOT IDSs

DL Techniques	Attack Types	Advantages	Disadvantages
RNN[19,20]	R2L, DoS, U2R, and Probe and predict the anomalies in time-series data	Best suited in a scenario where data is to be processed sequentially. The IoT device environment can generate sequential data in certain situations. As a result, RNNs are appropriate for IoT protection.	The most challenging aspect of using RNNs is dealing with vanishing or exploding gradients, which makes it challenging to learn long data sequences difficult.
CNN[18]	Malware attacks	CNN is ideally suited for extracting highly effective and fast features from raw data. CNN can learn behavior automatically from raw network security data, and they may be useful in IoT security.	CNN takes a lot of processing capacity, so using it for authentication on resource-constrained IoT devices is difficult.
Deep Autoencoders[21,22]	Malware attacks Botnet attacks	AEs have been used to extract features and reduce dimensionality with incredible results.	AEs are computationally powerful. and does not yield desired effects if the training dataset is not similar to the testing dataset
RBM [23]	R2L, DoS, U2R and Probe	RBMs' feedback feature makes it easier to retrieve essential attributes, which are then used to capture IoT traffic behavior.	RBMs require a lot of computational power, and they can be implemented on low-power IoT devices. A single RBM is incapable of representing features.
DBN[24]	R2L, DoS, U2R and Probe	With training on unlabeled data, it's ideal for extracting critical features.	DBNs require high computational costs.
GAN[25]	Botnet (Mirai, Bashlite), Scanning, MiTM	Detection of unknown threats.	It produces unstable results, and training is difficult
EDLN[16-25]	Malware, DoS, Botnet, MiTM	EDLNs perform better in an unpredictable scenario with prominent features, so an ensemble of DL classifiers will improve model efficiency.	EDLNs are computationally heavy and complex.

III. DATASET

This section discusses frequently used datasets in IoT networks for IDS are KDDCUP99, UNSW-NB15, and NSL-KDD. Table 3 gives an overview of the advantage and disadvantages of the most common datasets for the IDS evaluation. Then Fig.6 and Fig.7 shows the accuracy of the ML/DL Model on the NSL-KDD dataset.

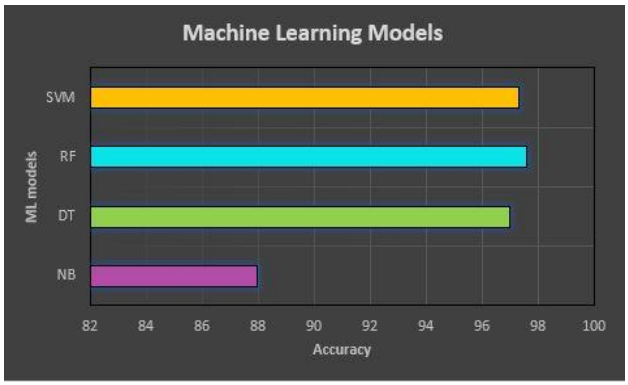

Fig.6. accuracy of the ML Model

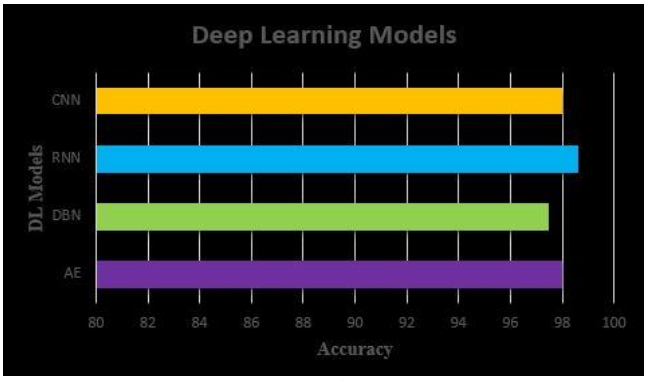

Fig.7. accuracy of the DL Model

The comparative study applied on the NSL-KDD dataset on binary classification, which had 41 attributes and one class attribute. The four categories of attacks are Denial of Service (DoS), Probe, Remote to Local (R2L). User to Root (U2R).

Table.3 IOT DATASET USED FOR IDS

DATASETS	ADVANTAGES	DISADVANTAGES
KDDCUP 99[26]	The dataset contains Labelled data. Based on 41 features for each connection, along with the class label. Implements Probing attacks, Denial of Service, User to Root, and Remote to User,	KDD99 suffers from unbalanced classification methods. Dataset does not contain updated attacks.
NSL-KDD [26]	Better than KDDCUP99 Overcome KDDCUP99 limitations	Lack of modern attack
UNSW-NB15[26]	Generate network traffic CSV files and (PCAP). It consists of nine types of attack, namely, Analysis, Fuzzers Backdoors, Dos, Reconnaissance, Exploit, Worms, Generic, and shellcode	It is complex than the KDD99 dataset due to the modern attack's similar behaviors and normal network traffic.

IV. CHALLENGES AND FUTURE SCOPE

Concerns regarding data security vulnerabilities are increasing with the development of IoT. The problem is that no standard framework exists that ensures the validation of the proposed systems. The research work primarily illustrates the estimation of their methods that has been presented in IoT systems based on their implemented datasets and discusses one particular issue that does not work on actual data in the real world and the presence of the other problems. It is challenging to develop an IDS that covers most of the essential aspects of an IDS, i.e., it is deployable, flexible, online, operates efficiently on actual data, and meets all stakeholders' specifications. Instead, much of the published literature shares the assessment test findings based on the constructed datasets, covers some or fixed parts of the method, and uses biased criteria to display results.

The most recent intrusion detection problems that occur in IoT networks are discussed:

It is demanding to create a real-time detection system for anomaly detection for IoT networks. This is because such an IDS will involve understanding normal behavior to predict suspicious or abnormal behavior first. The learning process implies no external attack or attack traffic that cannot be assured during this time. Such an IDS will produce high false alarms if these issues are not dealt with.

The various stages required in the designing and executing IDS, such as feature reduction, data preprocessing, and model preparation and implementation, in particular, ML/DL-based techniques for IDS, increase computation complexity. Constructing an effective IDS that is lightweight on computational requirements is another problem and field for future study.

To minimize future risks, it is considered that the need for further research that relies on threat detection becomes a reality in that sense and that their security issues, such as privacy and confidentiality, have been recognized and must be resolved and prevented.

V. CONCLUSION

The Internet of Things (IoT) has the ability to transform the future and get global things into our hands. Therefore, to improve security with time and increasing popularity, complexities, and security, IoT has become a widely explored area that needs to be resolved with new solutions and innovative strategic strategies for unpredictable attacks in the near future. This paper discussed various machine learning and deep learning methodologies for intrusion detection and their advantage and disadvantage, and the study showed that intrusion detection in the IoT is still having a problem. Most techniques can reduce the false positive rate so that training and the classification time increase. On the other hand, specific strategies execute the opposite method, i.e., if the false positive rate is stable, but the expense of a high statistical burden on training and research. Such a problem is of interest to intrusion prevention, where real-time detection is a relevant aspect. This study aims to give researchers a detailed summary of different security issues currently facing IoT systems and potential solutions, with an emphasis on intrusion prevention, focusing on ML/DL-based approaches.

REFERENCES

[1] Tabassum, Kahkashan, Ahmed Ibrahim, and Sahar A. El Rahman. "Security issues and challenges in IoT." In 2019 International Conference on Computer and Information Sciences (ICCIS), pp. 1-5. IEEE, 2019.

[2] Zarpelão, Bruno Bogaz, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84 (2017), pp. 25-37.

[3] Tahsien, Syeda Manjia, Hadis Karimipour, and Petros Spachos. "Machine learning-based solutions for the security of Internet of Things (IoT): A survey." Journal of Network and Computer Applications (2020), p.102630.

[4] Hussain, Fatima, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. "Machine learning in IoT security: Current solutions and future challenges." IEEE Communications Surveys & Tutorials 22, no. 3 (2020), p.1686-1721.

[5] Hajiheidari, Somayye, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour. "Intrusion detection systems in the Internet of things: A comprehensive investigation." Computer Networks 160 (2019), pp.165-191.

[6] Pajouh HH, Javidan R, Khayami R, Dehghantanha A, Choo KK "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks." IEEE Transactions on Emerging Topics in Computing. 2016 Nov 29;7(2), pp.314-23.

[7] Swarnkar, Mayank, and Neminath Hubballi. "OCPAD: One class Naive Bayes classifier for payload based anomaly detection." Expert Systems with Applications 64 (2016), pp.330-339.

[8] Bhati, Bhoopesh Singh, and C. S. Rai. "Analysis of support vector machine-based intrusion detection techniques." Arabian Journal for Science and Engineering 45, no. 4 (2020): 2371-2383.

[9] Y. Liu and D. Pi, "A Novel Kernel SVM Algorithm with Game Theory for Network Intrusion Detection," KSII Transactions on Internet & Information Systems, vol. 11, no. 8, 2017

[10] Goeschel, Kathleen. "Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis." In SoutheastCon 2016, pp. 1-6. IEEE, 2016.

[11] Doshi R, Apthorpe N, Feamster N. "Machine learning DDoS detection for consumer internet of things devices," In2018 IEEE Security and Privacy Workshops (SPW) 2018 May 24 (pp. 29-35). IEEE.

[12] Gaikwad DP, Thool RC. "Intrusion detection system using bagging ensemble method of machine learning." In2015 International Conference on Computing Communication Control and Automation 2015 Feb 26 (pp. 291-295). IEEE.

[13] Gao, Xianwei, Chun Shan, Changzhen Hu, Zequn Niu, and Zhen Liu. "An adaptive ensemble machine learning model for intrusion detection." IEEE Access 7 (2019) pp.82512-82521.

[14] Chandrasekhar, A. M., and K. Raghuveer. "Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers." In 2013 International Conference on Computer Communication and Informatics, pp. 1-7. IEEE, 2013.

[15] Zhao, Shengchu, Wei Li, Tanveer Zia, and Albert Y. Zomaya. "A dimension reduction model and classifier for anomaly-based intrusion detection in the internet of things." In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 836-843. IEEE, 2017.

[16] Li, He, Kaoru Ota, and Mianxiong Dong. "Learning IoT in edge: Deep learning for the Internet of Things with edge computing." IEEE network 32, no. 1 (2018), pp. 96-101.

[17] Fadlullah, Zubair Md, Fengxiao Tang, Bomin Mao, Nei Kato, Osamu Akashi, Takeru Inoue, and Kimihiro Mizutani. "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems." IEEE Communications Surveys & Tutorials 19, no. 4 (2017): 2432-2455.

[18] Vinayakumar, R., K. P. Soman, and Prabaharan Poornachandran. "Applying convolutional neural network for network intrusion detection." In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1222- 1228. IEEE, 2017.

[19] Torres, Pablo, Carlos Catania, Sebastian Garcia, and Carlos Garcia Garino. "An analysis of recurrent neural networks for botnet detection behavior." In 2016 IEEE biennial congress of Argentina (ARGENCON), pp. 1-6. IEEE, 2016.

[20] Almiani, Muder, Alia AbuGhazleh, Amer Al-Rahayfeh, Saleh Atiewi, and Abdul Razaque. "Deep recurrent neural network for IoT intrusion detection system." Simulation Modelling Practice and Theory 101 (2020): 102031.

[21] Mirsky, Yisroel, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai. "Kitsune: an ensemble of autoencoders for online network intrusion detection." arXiv preprint arXiv:1802.09089 (2018).

[22] Al-Qatf, Majjed, Yu Lasheng, Mohammed Al-Habib, and Kamal Al-Sabahi. "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection." IEEE Access 6 (2018): 52843- 52856.

[23] Mayuranathan, M., M. Murugan, and V. Dhanakoti. "Best features- based intrusion detection system by RBM model for detecting DDoS in cloud environment." Journal of Ambient Intelligence and Humanized Computing (2019), pp. 1-11.

[24] Li, Yuancheng, Rong Ma, and Runhai Jiao. "A hybrid malicious code detection method based on deep learning." International Journal of Security and Its Applications 9.5 (2015), pp. 205-216.

[25] Li, Dan, Dacheng Chen, Jonathan Goh, and See-kiong Ng. "Anomaly detection with generative adversarial networks for multivariate time series." arXiv preprint arXiv:1809.04758 (2018).

[26] Choudhary, Sarika, and Nishtha Kesswani. "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT." Procedia Computer Science 167 (2020): 1561-1573.