ISSN 2047-3338

Comparative Analysis of Machine Learning Algorithms for Intrusion Detection in IoT Environment

Hafsa Riaz[1], Anum Islam[2], M. J. Arshad[3]

[1,2,3]Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

[1]2021mscs560@student.uet.edu.pk, [2]2021mscs535@student.uet.edu.pk

***Abstract*– The cumulative number of connected devices in IoT environments has led to a corresponding increase in the number of security threats. For IoT networks and devices to be secure and private, intrusion detection is essential. In the Internet of Things, machine learning algorithms have become a promising intrusion detection method. However, there are several different machine learning algorithms to choose from, each with its own strengths and weaknesses. A comparison of frequently employed machine learning techniques for intrusion detection in IoT contexts is presented in this review study. The paper examines the strengths and weaknesses of each algorithm, including their ability to detect known and unknown attacks, their false positive rates, their computational efficiency, and their training data requirements. Several machines learning algorithms, including Support Vector Machines, Artificial Neural Networks (ANN), Logistic Regression (LR), Decision Trees (DT), K-Nearest Neighbour (kNN), Random Forest (RF), Naive Bayes, and Deep Learning, are examined in-depth in this paper. The analysis includes a discussion of the algorithms' performance in different use cases, as well as their potential limitations. The paper concludes with recommendations for selecting the best machine learning algorithm for intrusion detection in IoT environments. The recommendations consider the specific use case, available data, and other relevant factors. The paper provides valuable insights for organizations looking to improve their IoT security posture and protect their devices and networks from potential threats.**

***Index Terms*– Machine Learning Algorithms, Deep Learning, Iot Environment, Intrusion Detection, K-Nearest Neighbors and Logistic Regression**

I. INTRODUCTION

THE appellation "Internet of Things" (IoT) states to an assortment of internet-connected devices that exchange data automatically. These devices are typically linked to the cloud, as they generate a significant amount of data that requires processing. The IoT system is developed as a mix of several components, as shown in Fig. 1. The IoT system comprises several components, such as sensors, microcontrollers, wireless power, antennas, and more. These devices are connected to the cloud via a gateway, such as Bluetooth, ZigBee, Z-Wave, NFC, and others. The processing of the massive amounts of data produced by IoT devices, which must be organised and made comprehensible for analysis and forecasting, depends on the cloud. According to experts, there will be 24.1 billion IoT devices and a $1.5 trillion IoT market by 2030 [1].

In the IoT market, a major challenge we face is the vulnerability of IoT devices. This is partly because manufacturers often do not understand the significance of IoT security issues. Additionally, even when manufacturers are aware of security concerns, implementing security systems on devices may not be a priority due to cost constraints.

The IoT automated network system is becoming increasingly complex as demand and growth continue to surge [2]. This growth has been driven by the affordability of sensors, the rise of wireless connectivity, and cloud computing. With the advent of data-driven infrastructure, research has increasingly focused on the use of machine learning (ML) in conjunction with IoT [3]. IoT and ML techniques are used across numerous domains, including smart homes, industrial automation, healthcare, agriculture, smart cities, retail, and transportation. For example, in smart homes, IoT devices can automate various aspects of homes, such as lighting, temperature, and security, while in healthcare, they can be used to remotely monitor patients' health conditions. Despite the many benefits of IoT and ML applications, these systems' increasing complexity exposes them to unintended vulnerabilities, leading to security breaches and other anomalies. In addition, complex tasks such as interpreting ECG, detecting diseases using X-Ray, and analysing genomic data require the use of ML approaches. Even the aerospace industry can benefit from ML approaches. IoT devices are more prone to assaults since they are wireless [4]. Unlike attacks on local networks, which are frequently limited to adjacent nodes or a small local domain, assaults on IoT systems have the potential to spread over a greater area and have significant effects on IoT sites [5].

To safeguard against cybercrime, a secure IoT infrastructure will be crucial in the future. However, the vulnerability of IoT devices makes even the applied security measures susceptible to attack. For some stakeholders and business owners, data is their company's currency, and certain information is classified and sensitive for the government and commercial agencies. An IoT node's vulnerability can create a backdoor for attackers to collect sensitive data from any critical company [6].

As mentioned earlier, there are some straightforward solutions to address the challenges. In the signature-based approach [7], attacks and anomalies are saved in a database and tested against the database at regular intervals. However, this approach can be processing-intensive and is also susceptible to unforeseen dangers. IoT devices generate a vast amount of data, much of which includes sensitive information related to individuals, businesses, and smart cities.

To gain an understanding of the strengths and weaknesses of various machine learning algorithms used for intrusion detection in IoT environments, conducting a comparative analysis can provide valuable insights. This type of analysis can be useful for organizations to determine the most appropriate algorithm to use for their specific use case, as well as identify areas where further research is needed to enhance the effectiveness of intrusion detection systems in IoT environments. This process can help to improve overall IoT security posture, which is crucial for safeguarding devices and networks against potential threats.

The following sections will provide further analysis and comparison of other works in the field. In Section II, various research projects focused on IoT attacks and intrusion detection will be discussed. Section III will introduce the proposed taxonomy of IoT, including different types of attacks and anomalies. Section IV will focus on the learning models used in intrusion detection systems for IoT. Finally, Section IV will present conclusions and potential areas for future research.

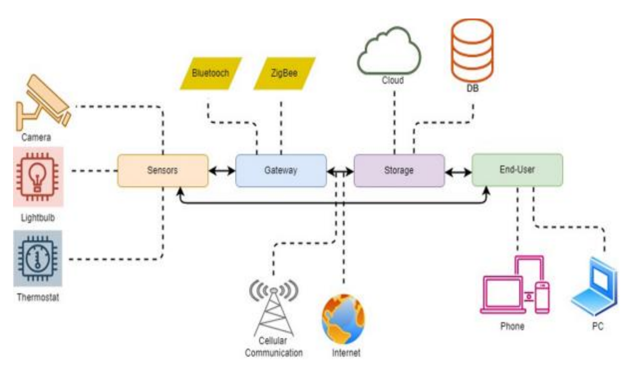

Fig. 1: IoT architecture [2]

II. RELATED WORK

Previous research in the field of IoT has shown promising results. For instance, Pahl et al. [8] developed an anomaly detection system and firewall for IoT microservices at IoT sites. In this work, clustering methods such as K-Means and BIRCH were used to group different microservices. The clustering model was updated using an online learning technique, and clusters were grouped if their centre was within three standard deviations distance. The overall accuracy achieved by the system with the implemented algorithms was 96.3%.

The research work done in the field of IoT has contributed to the development of several systems aimed at detecting security breaches [9]. For instance, in [11], a smart home system that used a deep learning approach with a Dense Random Neural Network (DRNN) to detect Denial of Service (DoS) and Denial of Sleep (DoS) attacks were described. The system relied on a set of metrics obtained from packet captures to predict the probability of a network attack. The authors provided a detailed account of the system's architecture and evaluation results, demonstrating the effectiveness of the approach.

In a study by Liu et al. [10], a detector was developed for On and Off attacks by malicious network nodes in an industrial IoT environment. These attacks take place when an IoT network is attacked by a malicious node while it is in an active or "On" state, yet the network functions correctly when the malicious node is in an inactive or "Off" state. To find abnormalities, the system employs a light probe routing technique and computes trust estimates for each neighbour node.

Diro et al. [2] investigated the fog-to-things architecture for threat detection. The authors of the article compared deep and shallow neural networks using an open-source dataset. This study's primary goal was to categorise four types of assault and abnormality. The achieved accuracy of for four distinct classes are: for shallow neural networks (SNN) of 96.75% and deep neural networks (DNN) of 98.27%.

The security issues that arise when creating embedded technologies for the Internet of Things (IoT) were discussed by Usmonov and colleagues in a recent study [12]. A significant problem was recognized as preserving data integrity when transferring data among physical, rational and virtualized components of an IoT system. The authors of the paper recommended using digital watermarks to address these difficulties.

Anthi et al. [13] proposed an intrusion detection system for the Internet of Things (IoT). The study employed multiple machine learning (ML) classifiers to effectively detect network scanning probing and elementary types of Denial of Service (DoS) attacks. The data set for the study was generated by capturing network traffic over four continuous days using Wireshark software. The ML classifiers were applied using the Weka software.

In their research, Ukil et al. [14] focused on identifying anomalies in healthcare analytics utilizing the Internet of Things (IoT). The study introduced a cardiac anomaly detection model that can be utilized through a smartphone. The authors used distinct types of methods, including IoT sensors, biomedical signal analysis, predictive analytics, medical image analysis and big data mining to find abnormalities in healthcare.

A two-layer dimension reduction and two-tier classification module are used in Pajouh at al.'s [15] suggested intrusion detection model to identify malicious operations like User to Root (U2R) and Remote Local (R2L) assaults. The experiment made use of the NSL-KDD dataset, and dimension reduction was accomplished using component analysis and linear discriminate analysis. (U2R) and Remote Local (R2L) attacks. The study employed component analysis and linear discriminate analysis for dimension reduction and the NSL-KDD dataset for the experiment.

The binary NSLKDD dataset and Real Traffic Data from Federico II University of Napoli were both analysed in this paper by Angelo at el. [16] using the Uncertainty-managing Batch Relevance-based Artificial Intelligence (U-BRAIN) technique. The U-Brain model works dynamically across numerous computers and can handle missing data. The authors used the J-48-based classification method to choose 6 features from the NSL-KDD dataset's total of 41 features. For NSL-KDD and Real Traffic Data, respectively, the study reported accuracy rates of 94.1% and 97.4% (10-fold training mean).

Kozik et el. [17] suggested a cloud architecture-based classification-based threat detection service that makes use of HPC cluster resources for labour- and cost-intensive classifier training. The Extreme Learning Machines (ELM) classifier, which enables effective computations and analysis of gathered data in edge computing environments, was the subject of the study. Its structure and characteristics were examined. Three IoT system scenarios—scanning, infected host and command and control —were the main focus of the effort. For each of these cases, the research reported accuracy ratings of 0.99, 0.76, and 0.95.

III. COMPARATIVE ANALYSIS

This section presents performance measures including intrusion detection accuracy (IDA), datasets, machine learning (ML) algorithms, threats, and purpose to analyse the effectiveness of several existing intrusion detection technologies. Table I compares the proposed IoT attack detection method with state-of-the-art methods. Table II lists the sources, traffic categories, characteristics, feature types, and anomalies for several incursion datasets.

Table I: A comparison of the suggested IoT attack detection method with the state of the art.

Reference	Year	Method	Dataset	Purpose	Attacks	Accuracy
Pahl et al. [3]	2003	KNN BIRCH	Own Synthetic	a firewall and detector for IoT microservice anomalies		96.3%
Pereira et al. [4]	2012	Optimum-Path Forest (OPF)	NSL-KDD	Ability of computer network to detect intrusions	Normal DOS R2L U2R Probing	94%
D'Angelo et al. [5]	2015	U-Brain	NSL-KDD Real Traffic Data	A batch relevance-based method for controlling uncertainty for network anomaly detection	Network Anomalies	94.1% 97.4%
Ukil et al. [6]	2016		Own Synthetic	detection of anomalies in healthcare		N/A
Usmonov et al. [7]	2017		Own Synthetic	security problem during developing embedded technologies		N/A
Bostan et al. [8]	2017	Optimum-Path Forest Clustering, SA-IDSs	Own Synthetic	Real-time hybrid intrusion detection system that is innovative	sinkhole Selective-forwarding blackhole wormhole rank	96.02%
	2017	Random Forest	NSL-KDD		Normal	99%

Lopez-Martin et al. [9]		Linear SVM		Conditional Variational Autoencoder for Prediction and Feature Recovery in IoT Intrusion Detection	DOS	92%
		Multinomial			R2L	65%
					U2R	
					Probing	
Brun et al. [10]	2018	DRNN	Real time series own synthetic data	Attacks on IoT-connected home environments: Detection	DOS (Denial of service)	N/A
					DOS (Denial of Sleep)	
Liu et al. [11]	2018	TLPD (trust joint light probe-based defense mechanism)	Own Synthetic	detector for malicious network node attacks that occur both on and off at an industrial IoT site	On & OFF attack	I.R. = 0.80(>)
Diro et al. [2]	2018	deep neural network model	NSL-KDD	Fog-to-things architecture for distributed deep learning-based IoT/Fog network attack detection	Normal	98.27%
					DOS	
		shallow neural network model			R2L	96.75%
					Probing	
					U2R	
Anthi et al. [12]	2018	Naive Bayes	Own Synthetic	an IoT intrusion detection system	DOS	N/A
					Probing	
Kozik et al. [13]	2018	ELM	CTU	threat detection service using cloud architecture in an edge computing environment that is based on the classification	DOS by several kind of botnets	N/A
Pajouh et al. [14]	2019	Naive Bayes	NSL-KDD	Based on a two-layer dimension reduction and two-tier classification module, intrusion detection	U2R	I.R. = 84.82
		Certainty Factor version of KNN			R2L	
Hasan et al. [15]	2019	LR	DS2OS Traffic traces	IoT sensor attack and anomaly detection	DOS	98.3%
		SVM			Datatype Probing	98.2%
		DT (Decision Tree)			Scan	99.4%
					Wrong Setup	
		RF (Random Forest Trees)			Malicious Control	99.4%
					Spying	
		ANN			Malicious Operation	99.4%
Soodeh Hosseini, B. M. H. Zade [16]	2020	NSL-KDD	MGA-SVM-HGS-PSOANN	employing a new hybrid approach that combines evolutionary algorithms, SVM, and ANN to detect attacks		99.3%
Ashfaq and Juntae	2020	CSE-CICIDS2018	Spark MLlib, Conv-AE	Conv-AE-Based Intrusion Detection System Development Using Heterogeneous Dataset	Zero-day attacks	98.20%
YUFENG, PENJ [17]	2021	DBN	CSE-CICIDS2018	Deep Belief Network-Based Intrusion Detection Classification Model Optimization	Zero-day attacks	95%
Ashfaq [18]	2021	GA,Fuzzy	NSL-KDD	Network intrusion detection system using hybrid convolutional recurrent neural networks, or HCRNNIDS.		99.96%
Acharjya et al. [19]	2021		Own-synthetic	Elderly Perception on the Internet of Things-Based Integrated Smart-Home System		
John et al. [20]	2022	Gaussian Naïve-Bayes	UNSW-NB15	Comparative analysis of intrusion detection using ML and DL approaches	Cyber attacks	51.57%
		Decision Tree	Kyoto			95.86%
		Stochastic Gradient	NSL-KDD			97.14%
		Random Forest	KDDCUP			99.65%
		Non-Linear SVM				99.06%
		Linear SVM				97.13%
		Logistic Regression				96.69%
		Multilevel Perceptron				97.51%
		Gradient Boosting				99.61%
		K-Nearest Neighbour				99.33%
		Artificial Neural Network				98.5%
		Recurrent Neural Network				97.62%
		Convolutional Neural Network				98.95%
Baraa I. Farhan, Ammar D. Jasim [21]	2022	CSECIC-IDS2018	DL models	A survey of intrusion detection from the perspective of	Malicious attacks	

		Bot-IoT		intrusion datasets and machine learning techniques		
Kumar,selvi and kannon [22]	2023	Fuzzy CNN algorithm	KDD cup 1999	An in-depth analysis of machine learning-based intrusion detection systems for encrypted communication in the Internet of Things	Normal	
					DOS	97%
					DoS-synfooding	92%
					R2L	94%
					Probing	98.2%
					U2R	
					ARP fooding	
					HTTP fooding	
					UDP fooding	
Chaganti, Rajasekhar and Suliman [23]	2023	DNN	DS1	Deep Learning Approach for IoT Networks' SDN-Enabled Intrusion Detection System	DDOS	97%
		CNN	DS2			96%
		LSTM				97%
ElKashlan, Mohamed and Elsayed [24]	2023	Naïve Bayes classifier	IoT-23	Electric vehicle charging stations (EVCSs) for the Internet of Things with an autonomous learning-based intrusion detection system	DDOS	86.7%
		J48 classifier			Benign	97.4%
					C&C	
		Filtered classifier			Okiru	99.2%
					Part of a horizontal port scan	
Ayesha S. Dina, A.B. Siddique, D. Manivannan [25]	2023	FNNs	Bot-IoT	Using the focus loss function, a deep learning technique to intrusion detection in the Internet of Things	DDOS	
			WUSTL-IIoT-2021			
		CNN	WUSTL-EHMS-2020			
He, Ke and Kim, Dan Dongseong and Asghar, Muhammad Rizwan [26]	2023	DNN		A Comprehensive Survey of Adversarial Machine Learning for Network Intrusion Detection Systems	White-box adversarial attacks	
					black-box adversarial attacks	
Santhanakrishnan [27]	2023	CNN	Own-synthetic	Intrusion Detection System to Detect Anomalies using Convolution Neural Network in IO	DOS	96.9%
					Replay	
					DDOS	
					Spoofing	

Table II: Comparative description of intrusion datasets

Datasets	Source	Category	Features	Feature-Type	Anomalies
KDD Cup 99	Preprocessed DARPA 1998 data produced in MIT Lincoh Laboratory	Simulated/Synthetic Data	41	Categorical	DoS-back, land Neptune, pod, smurf, teardrop
				Binary	U2R-buffer_overflow, loadmodule, Perl, rootkit
				Discrete	R2Lftp_write, phf, spy, guesspassword, imap. multihop, warezlient, warezmaster
				Continuous	Probe-ipsweep, nmap, portsweep, satan
NSL-KDD	Upgraded sort of KDD Cup99	Simulated/Synthetic Data	42	Categorical	DoS-back, land Neptune, pod, smurf, teardrop
				Binary	U2R-buffer_overflow, loadmodule, Perl, rootkit
				Discrete	R2Lftp_write, phf, spy, guesspassword, imap. multihop, warezlient, warezmaster
				Continuous	Probe-ipsweep, nmap, portsweep, satan
AWID	Real traces of a dedicated WEP protected 802.11 network	Real trace 802.11 WiFi networks. WLAN traffic in packet-based format	155	Categorical	Flooding
				Continuous	
				Hexadecimal	Impersonation
				Discrete	Injection
S5	Yahoo Labs Media Sciences team	Real and simulated time series data	Class A1, A2-3 features	Time series data	Outliers
			Class A3, A4-9 features		change-point
NAB	Real data AWS Server, traffic data, twitter advertisement Artificially generated data	Simulated and real-world streaming data First temporal benchmark	116 columns in 58 csv file include 58 datetime	Ordered timestamped	Spatial Anomaly
			42 decimal and 16 integer columns	Single-valued metrics	Temporal Anomaly

Kyoto 2006+	Kyoto University's Honeypots	Real traffic data from different honeypots	24 (14 conventional and 10 additional features)	Categorical Discrete Continuous	Abnormal, unknown
UNSW-NB15	Cyber Range Lab of Australian Center for Cyber Security	Real modern normal network traffic activities Contemporary synthesized attack traffic activities	49	Categorical Binary Discrete Continuous	Generic Worms Backdoor DoS Exploits Fuzzers Reconnaissance Shellcode
Bot_IoT	Research Cyber Range Lab of UNSW Canberra	Real and simulated IoT network traffic	46	Categorical Binary Discrete Continuous	Information gathering: OS and service scan DDoS DOS Information theft: Keylogging and Data theft
Genome	National Science Foundation, USA	1260 samples of android malware	26	Binary	49 malware families
Drabin	Mobile Sandbox Project	123,453 benign applications and 5560 malware samples	545,333		179 different malware families
Contagio	Deep End Research Project by Mila Parkour	11960 mobile malware samples and 16800 benign samples	Sorted malicious and clean files of different categories		Total malware- 189

IV. INTRUSION DETECTION SYSTEMS FOR IOT COMMUNICATION

The Intrusion detection system classification in IoT is presented in Figure 2. It can be alienated into three classes: topology-based IDS, attack-based IDS, and IDS based on the intrusion detection technique used [14]. The intrusion detection technique is further divided into four categories: hybrid IDS, anomaly IDS, specification IDS, and signature IDS. The network structure-based IDS is classified into CIDS, DIDS, and HIDS. In addition, IDS for detecting specific types of attacks such as denial of service, wormhole, Sybil, false data injection, reply, and jamming attacks can also be identified.

Machine Learning Algorithms: Machine learning is a branch of research that entails developing computational algorithms that mimic human learning processes to acquire knowledge automatically. It is an interdisciplinary field that involves computer science, statistics, psychology, and neuroscience [34]. The algorithms employed in machine learning are categorized into three groups based on learning approaches, namely supervised learning, unsupervised learning, and reinforcement learning. Fig. 2 illustrates the types of machine learning (ML) algorithms.

The overall framework of machine learning consists of several independent processes, as shown in Figure 3. The first process is data assemblage and observation, where the dataset is carefully collected and observed to identify the type of data. Data pre-processing is then performed on the dataset, which includes visualization, data cleaning, feature engineering, and vectorization to convert the information into feature vectors. These feature vectors are then split into a training and testing set in an 80:20 ratio. In the learning algorithm, the training set is used to build a final model using an optimization strategy. Various optimization strategies were applied in this work for different classifiers.

Support Vector Machine (SVM): Support Vector Machine (SVM) is a sort of discriminative model that is similar to logistic regression. It is a supervised learning model that is frequently employed for regression, classification, and outlier detection [25], [26]. SVM is particularly useful for analyzing nonlinear data [36].

Decision Tree (DT): Decision Tree is a form of algorithm that enables nodes to assess different actions by weighing their costs, benefits, and probabilities.

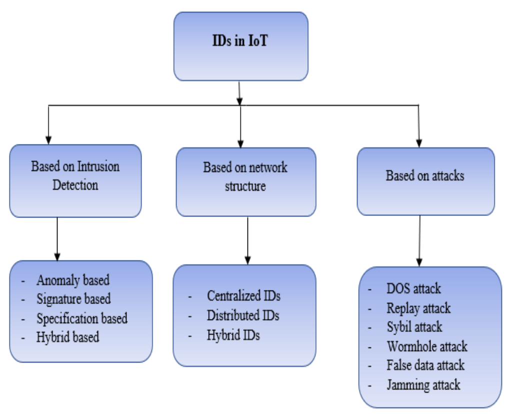

Fig. 2: Taxonomy of IoT

Essentially, it provides a roadmap of possible outcomes stemming from a series of connected choices. It usually starts with just one node and branching out into numerous results, each of which leads to other nodes and more branches. As a result, it resembles a tree-like structure or a flowchart [28], [37].

Logistic Regression (LR): Logistic Regression (LR) is a sort of discriminative model that is dependent on the dataset's quality. Logistic regression is a quantitative analytic approach that uses previous assessments of a data set to predict a binary result, such as yes or no. A logistic regression model forecasts a dependent variable by examining the connection amongst one or more pre-existing independent variables.

Naive Bayes (NB): Naive Bayes is a popular machine-learning algorithm used for classification tasks. Based on past knowledge of circumstances that could be relevant to the occurrence, Bayes' theorem is used to determine the likelihood of an event. Naive Bayes makes the assumption that each feature's existence or absence stands alone and is unrelated to each other.

This assumption is known as the "naive" assumption and while it may not always hold, it simplifies the computation and can make the algorithm more efficient [41].

Random Forest (RF): The random forest method generates a forest with several decision trees as part of its supervised classification process.

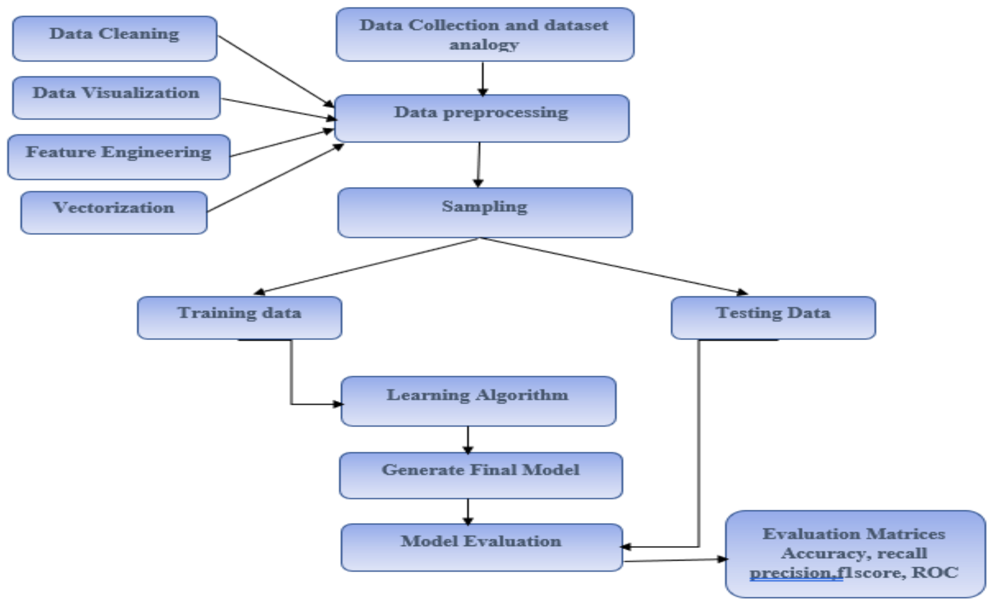

Fig. 3: Overall framework for attack detection in IoT

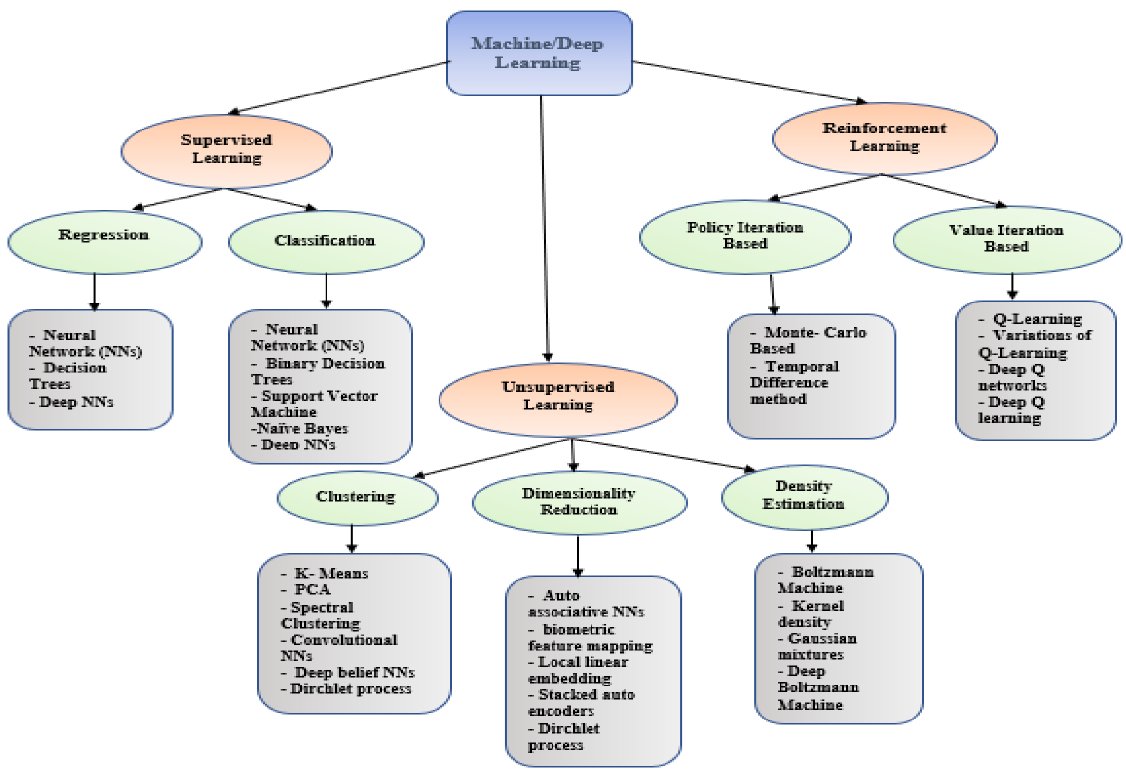

Fig. 4: Family of Machine Learning

The name comes from the fact that each tree is created randomly, with slight variations in the feature set and data used. The algorithm then averages the predictions of each tree to make a final prediction. Due to its ensemble approach, the random forest algorithm typically has higher predictive accuracy than a single decision tree. Additionally, it is known for its high execution speed, making it an attractive option for large datasets. As a population of random forest grows, its performance typically gets better [30], [38].

Deep Recurrent Neural Network (DRNN): The Deep Recurrent Neural Network (DRNN) is a type of neural network architecture that integrates the concepts of deep learning and recurrent neural networks (RNNs). DRNNs have a feedback loop like RNNs, which helps them process sequential data. This feedback loop enables the network to maintain a state or memory of past inputs, which is essential for tasks such as natural language processing or speech recognition. DRNNs also have multiple layers of neurons, allowing them to learn hierarchical representations of the input data. This characteristic is shared with deep learning neural networks, which can learn complex features by hierarchically combining simpler ones [40]. Artificial Neural Network (ANN): A deep learning algorithm's foundation is an artificial neural network (ANN), a machine learning approach. Raw data may be used to train the ANN model. In contrast with other classifiers, it contains more tuning parameters, making it a more sophisticated structure. Additionally, it takes more time than other methods to optimize the error. As a result, CUDA programming is used to train instances of neural network algorithms on the graphics processing unit (GPU). A feature set X = X1, X2, X3, ..., Xn (where X1 - Xn = unique characteristics) is trained on each neuron node of the ANN. The features are added with bias values, b = b1, b2, ..., bn, and multiplied by random weights, W = W1, W2, W3, ..., Wn. A non-linear activation function is then fed the obtained values as input [39].

V. CONCLUSIONS

This study found that intrusion detection is still difficult in the setting of the Internet of Things. The emphasis moves from connectivity to data as the Internet of Things (IoT) develops. In order to keep data safe, this effort concentrated on the most recent research in intrusion detection and intelligent IoT approaches. The works examined in this research largely covered the concern and numerous attempts put forward by researchers and the industry centered on the creation of optimized security procedures that deliver adequate protection.

The study also includes a number of clever approaches that are applied to intrusion detection and network security in computer networks. Although these methods aim to increase intrusion detection recognition rates, it is believed that the false positive rate will continue to be a problem that needs to be addressed in all studies. While some techniques can decrease the false positive rate, they also require more training and classification. However, some methods reverse the process, stabilizing the false positive rate at the expense of high computational expenses for training and testing. This problem is extremely important for intrusion detection, because real-time detection is an important consideration.

REFERENCES

[1] 19 MAY 2020. [Online]. Available: https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030.

[2] A. A. D. a. N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems,* vol. 82, pp. 761-768, 2018.

[3] C. C. A. a. P. S. Y. a. J. H. a. J. Wang, "A Framework for Clustering Evolving Data Streams," in *Proceedings 2003 VLDB Conference*, San Francissco, Morgan Kaufmann, 2003, pp. 81-92.

[4] C. R. P. a. R. Y. N. a. K. A. C. a. J. P. Papa, "An Optimum-Path Forest framework for intrusion detection in computer networks," *Engineering Applications of Artificial Intelligence,* vol. 25, pp. 1226-1234, 2012.

[5] G. D. a. F. P. a. M. F. a. S. Rampone, "An uncertainty-managing batch relevance-based approach to network anomaly detection," *Applied Soft Computing,* vol. 38, pp. 408-418, 2015.

[6] A. a. B. S. a. P. C. a. P. A. Ukil, "IoT Healthcare Analytics: The Importance of Anomaly Detection," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 994-997.

[7] B. a. E. O. a. I. A. a. S. A. a. I. A. a. M. R. Usmonov, "The cybersecurity in development of IoT embedded technologies," in *2017 International Conference on Information Science and Communications Technologies (ICISCT)*, 2017, pp. 1-4.

[8] H. B. a. M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Computer Communications,* vol. 98, pp. 52-71, 2017.

[9] M. a. C. B. a. S.-E. A. a. L. J. Lopez-Martin, "Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT," *Sensors,* vol. 17, 2017.

[10] O. a. Y. Y. a. G. E. a. K. Y. M. a. A.-G. J. a. R. M. Brun, "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments," in *Security in Computer and Information Sciences: First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers 1*, 2018, pp. 79-89.

[11] X. a. L. Y. a. L. A. a. Y. L. T. Liu, "Defending ON–OFF Attacks Using Light Probing Messages in Smart Sensors for Industrial Communication Systems," *IEEE Transactions on Industrial Informatics,* vol. 14, pp. 3801-3811, 218.

[12] E. a. W. L. a. B. P. Anthi, "Pulse: An adaptive intrusion detection for the Internet of Things," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1-4.

[13] R. K. a. M. C. a. M. F. a. F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *Journal of Parallel and Distributed Computing,* vol. 119, pp. 18-26, 2018.

[14] H. H. a. J. R. a. K. R. a. D. A. a. C. K.-K. R. Pajouh, "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,* vol. 7, pp. 314-323, 2019.

[15] M. H. a. M. M. I. a. M. I. I. Z. a. M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things,* vol. 7, p. 100059, 2019.

[16] S. H. a. B. M. H. Zade, "New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN," *Computer Networks,* vol. 173, p. 107168, 2020.

[17] Y. L. Z. Z. H. L. D. L. PENG WEI, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," 2021.

[18] M. A. Khan, "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System," *Processes,* vol. 91, 2021.

[19] T. H. a. M. J. H. a. C. S. H. Jo, "{Elderly Perception on the Internet of Things-Based Integrated Smart-Home System," *sensors,* vol. 21, 2021.

[20] J. a. A. M. Note, "Comparative Analysis of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms," *Annals of Emerging Technologies in Computing,* vol. 6, pp. 19-26, 2022.

[21] A. D. J. Baraa I. Farhan, "Survey of Intrusion Detection Using Deep Learning in the Internet," *Journal for Computer Science and Mathematics,* 2022.

[22] M. S. ,. A. K. S. V. N. Santhosh Kumar, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Computational Intelligence and Neuroscience,* pp. 1687-5265, 2023.

[23] R. a. S. W. a. R. V. a. D. A. Chaganti, "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks," *Information,* vol. 14, 2023.

[24] M. a. E. M. S. a. J. A. D. a. A. M. ElKashlan, "A Machine Learning-Based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCSs)," *Electronics,* vol. 12, 2023.

[25] A. S. D. a. A. S. a. D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," *IoT,* vol. 22, p. 100699, 2023.

[26] K. a. K. D. D. a. A. M. R. He, "Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey," *{IEEE Communications Surveys & Tutorials,* vol. 25, pp. 538-566, 2023.

[27] J. S. S. R. M. A. S. R. M. Santhanakrishnan C, "Intrusion Detection System to Detect Anomalies using Convolution Neural Network in IOT," *Journal of Survey in Fisheries Sciences (SFS),* vol. 10, 2023.

[28] T. a. C. R. a. C. N. "Bhattasali, "Study of Security Issues in Pervasive Environment of Next Generation Internet of Things," in *Computer Information Systems and Industrial Management*, Berlin, Heidelberg, Springer Berlin Heidelberg, 2013, pp. 206-217.

[29] I. L. Sara Najari, "Malware Detection Using Data Mining Techniques," *International Journal of Intelligent Information Systems,* vol. 3, no. 6-1, pp. 33-37, 2014.

[30] D. S. Zeljko Gavric, "Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks," vol. 38, pp. 130-138, 2018.

[31] J. a. S. E. a. S. D. a. P. A. Newsome, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Association for Computing Machinery, 2004.

[32] M.-O. a. A. F.-X. Pahl, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," in *2018 14th International Conference on Network and Service Management (CNSM),* 2018, pp. 72-80.

[33] J. a. X. Y. a. C. C. P. Liu, "Authentication and Access Control in the Internet of Things," in *2012 32nd International Conference on Distributed Computing Systems Workshops,* 2012, pp. 588-592.

[34] J. a. S. N. a. K. K. Milosevic, "Malware in IoT software and hardware," 2016.

[35] W. Ding, "Study of Smart Warehouse Management System Based on the IOT"," in *Intelligence Computation and*

Evolutionary Computation, Berlin, Heidelberg, Springer Berlin Heidelberg, 2013, pp. 203-207.

[36] A. A. D. a. N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761-768, 2018.

[37] X. a. L. Y. a. L. A. a. Y. L. T. Liu, "IEEE Transactions on Industrial Informatics," *Defending ON–OFF Attacks Using Light Probing Messages in Smart Sensors for Industrial Communication Systems,* vol. 14, pp. 3801-3811, 2018.

[38] H. H. a. J. R. a. K. R. a. D. A. a. C. K.-K. R. Pajouh, "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,* vol. 7, pp. 314--323, 2016.

[39] H. H. a. J. R. a. K. R. a. D. A. a. C. K.-K. R. Pajouh, "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,* vol. 7, pp. 314--323, 2016.

[40] A. A. D. a. N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761-768, 2018.

[41] I. K. P. a. R. S. Sherratt, Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people, 2018.