Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADVANCEMENTS IN INTRUSION DETECTION SYSTEMS FOR INTERNET OF THINGS: A STATE-OF-THE-ART AND COMPREHENSIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS

RACHID HDIDOU[1], MOHAMED EL ALAMI[2]

[1,2]ERMIA Team, Department of Mathematics and Computer Science, National School of Applied Sciences Tangier, Abdelmalek Essaadi University, Morocco

E-mail: [1]hdidou.rachid@etu.uae.ac.ma, [2]m.elalamihassoun@uae.ac.ma

ABSTRACT

The Internet of Things is one of the technologies that form the basis of the modern technological revolution. The use of this technology in various fields has become a necessity due to development and the speed with which the world is changing. This use depends on and is linked with the resolution of some issues that impact the technology of the Internet of Things, among these issues, is the issue of security. Internet of Things computer security is considered one of the important points in the sustainable and secure use of Internet of Things technology in most fields, especially sensitive fields such as the medical field, the military field, the banking field, and other fields. Intrusion detection systems are considered one of the appropriate techniques to secure networks and IoT applications due to their flexibility in application. However, with the great development of cybercrime, the standard solutions of intrusion detection systems have become insufficient to secure applications and networks of the Internet of Things. This confirms the need to propose and develop intrusion detection system solutions based on artificial intelligence and machine learning techniques. In this paper, we will present a state-of-the-art and analytical study on Internet of Things security using intrusion detection system solutions based on Machine Learning algorithms.

Keywords: *Intrusion Detection Systems, Internet of Things, Machine Learning Algorithms, IDS, IoT.*

1. INTRODUCTION

In our present time, connecting to the Internet and obtaining an IP address is no longer limited to phones and computers. We have reached, however, a stage where everything, including people, animals, cars, and other objects can connect to the Internet through sensors and microchips, and those things can also send and receive information without human intervention, and this is referred to as the Internet of Things.

The concept of connected objects has appeared since the 1990s with many ideas, but the first appearance of the term Internet of Things dates to 1999 by the scientist Kevin Ashton during one of his presentations in Procter & Gamble (P&G) [1]. Moreover, the use of the Internet of Things developed at the beginning of the 2000s, especially with the appearance and development of artificial intelligence technologies, cloud computing, 4G, 5G, IPv6 technologies, big data, and other technologies.

Recently, the Internet of Things has become one of the widely used technologies to create and develop services in many fields [2], including:

Healthcare: The Internet of Things is used in data collection and continuous remote monitoring of patients using electronic chips and smart wearables.

The field of smart cities: The Internet of Things can be used in smart homes, to switch off lights or lock doors, and the Internet of Things is also used to create smart traffic lights, Traffic inside smart cities can be monitored and controlled by smart cameras linked to data centers.

The environmental field: There are many uses of the Internet of Things in the environmental field, starting with automatic watering of crops, passing through knowledge and monitoring of the weather, and ending with the monitoring of forests against fire and monitoring of water leaks.

The increasing use of the Internet of Things in most areas requires providing solid and effective

solutions to secure this technology. Internet of Things security requires the protection of applications, infrastructure, communication, and data [3].

Intrusion detection systems are defined as security systems that monitor the flow of data in the network, analyze that data, and identify normal and dangerous data. These systems are among the techniques that many researchers in the field of Internet of Things technology security are working on to provide solutions that are suitable and compatible with the structure of Internet of Things applications and networks.

In recent years, the world has witnessed a rise in sophistication of hacks and cyber-attacks with the increasing use of Internet of Things technology. As a result, interest in finding security solutions that are fast and more efficient, such as Intrusion Detection Systems known for their flexibility to use and ability to adapt, has increased. One of the modern technologies extensively used to enhance the quality and precision of Intrusion Detection Systems is Machine learning. Here we can post and list the following questions: What is the current state of advancement in scientific research on the use of Intrusion Detection Systems based on machine learning techniques to secure networks and Internet of Things applications? Have machine learning techniques been able to solve problems of Intrusion Detection Systems? What are the most effective machine learning algorithms for Intrusion Detection?

The rest of this work is structured as follows: Section II contains a brief presentation on the terms relating to our subject. Section III provides an overview of the work related to our research. Section IV contains a detailed state of the art while in section IV an analysis and discussion are presented. Finally, in section V, a conclusion and our future work are stated.

2. RELATED TERMS

2.1 Internet of Things (IoT)

The Internet of Things can be defined as a network of physical objects [4] capable of obtaining an IP address and connecting to the Internet on one hand and communicating with each other on the other. These objects can also send and receive data via sensors and chips, without human intervention.

The working mechanism of the Internet of Things can be divided into four layers [5]:

Sensors: The role of sensors lies in collecting data from where they are. There are several types of sensors: such as temperature sensors, humidity, gas, movement, and many other sensors of other variables.

The IoT Gateway: Its main role is manifested in collecting data from the various sensors within the internal network and transferring the data collected to the external network (Internet). Gateways can be considered mediators between the internal network of objects and the Internet.

Cloud Server: The data transferred by the Gateways is transferred and stored inside a server, to be processed and analyzed to make decisions automatically and intelligently.

Mobile App: This stage is considered the last stage of the Internet of Things mechanism, where all the data that has been collected, converted, and analyzed is available to the end user on his computer or his phone through an app, program, or website, and so he can make the appropriate decision and control the devices with a simple combination of button clicks.

The following diagram summarizes the functioning mechanism of the Internet of Things:

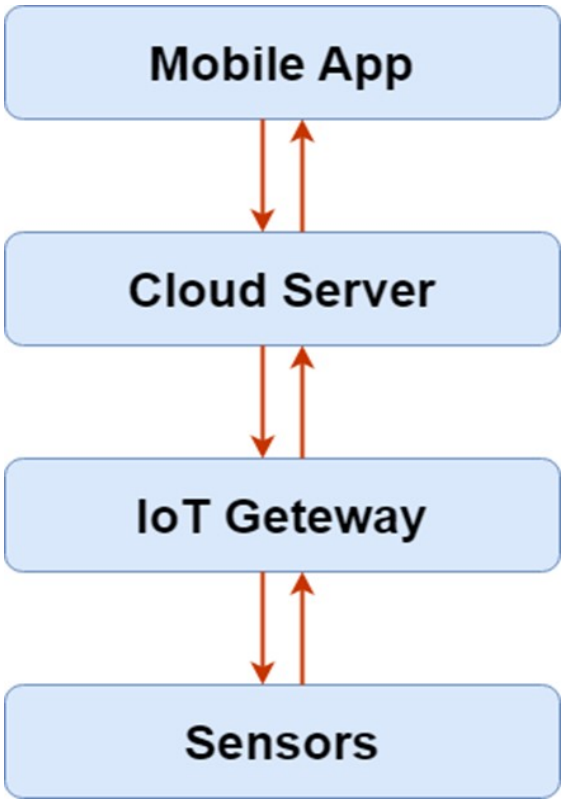

Figure 1: The working mechanism of IoT

2.2 Intrusion Detection Systems (IDSs)

An intrusion detection system is a computer system that monitors and analyzes the data flow in a network to identify malicious activity and report it to the network administrator.

There are two types of IDSs [6]:

NIDS: This type monitors the entire network by analyzing incoming and outgoing data traffic to the network, and acts as an intermediary between network devices and the Internet.

HIDS: In this type, the IDS is placed in the device itself and its main role is to monitor the device on which it is installed.

Based on the detection methodology, IDSs are further divided into two categories [7]:

The first category is a signature-based intrusion detection system. This type of IDS is based on the detection of signature attacks that is to say, if a signature of an attack is detected, the IDS sends an alert to the network administrator.

The second category is the anomaly intrusion detection system. In this type, the IDS is not based on signatures, but on behaviors, i.e., this type of IDS needs a learning step to identify the normal behavior of a network, and based on this behavior IDS detects abnormal behavior in the detection step.

2.3 Machine Learning (ML)

Machine Learning: It is a part of artificial intelligence that allows computer machines (computers, robots, Phones, etc.) to be given the ability to learn automatically from data rather than by implicit programming. Several definitions of machine learning have been proposed. In 1959 Arthur Samuel described machine learning as "a field of study that gives computers the ability to learn without being explicitly programmed". Another definition proposed by Tom M. Mitchell in 1997, this definition was in the form of the following situation “A computer program is said to learn from experience E with respect to some class tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E.”

Machine learning algorithms are organized into taxonomies, based on the desired outcome of the algorithm, the following Figure 2 summarizes the common algorithm types:

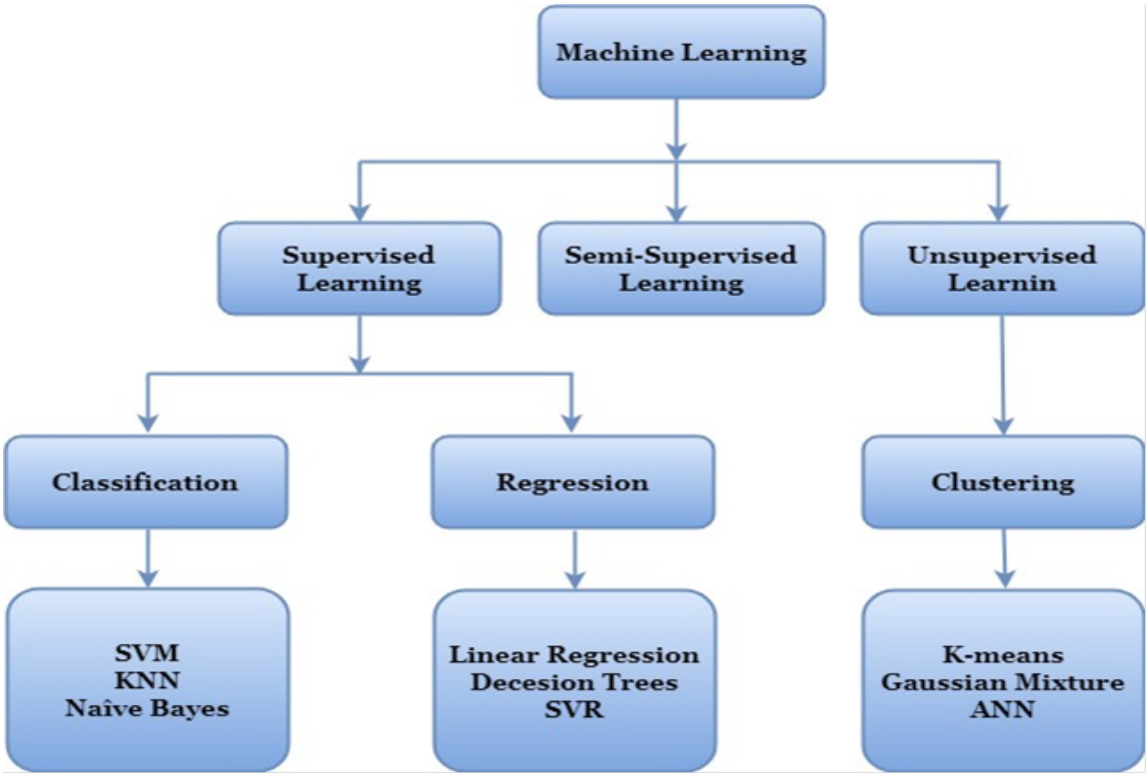

Figure 2: Types of Machine Learning Algorithms

- **Supervised Learning**

Supervised Learning: It is an approach to Machine Learning in which the machine is trained using samples of labeled data [8]. In this type of learning, the input and output data are known [9].

This type of learning contains two subtypes, which are classification and regression:

Classification: This is a machine learning technique that predicts whether data instances belong to a specific group (data class). We talk about classification when the outputs are classes, and when the values used are discrete.

Regression: It is another machine learning technique that makes it possible to distinguish data in continuous real values from the classification that uses classes. When we talk about an output variable in the form of a real or continuous value, we can talk about regression.

- **Unsupervised Learning**

Unsupervised Learning: It is an approach of Machine Learning in which the machine is trained using data samples that do not have labels [8]. This type of learning is the opposite of Supervised Learning, i.e. in Unsupervised Learning only the input data is known. This type of learning is used in the concept of clusterization [9].

Clustering: It is a machine learning technique that allows data to be divided into a certain number of groups, based on the similarity and dissimilarity between the data in a collection. Clustering is very important because the main clustering can be determined from unlabeled data. There is no specific criterion to choose the right Clustering to use.

- **Semi-Supervised**

It is a type of learning that combines the two previous types, i.e. it uses labeled samples and unlabeled samples to build an appropriate mapping.

3. RELATED WORKS

In 2018 Nadia Chaabouni et al [10], presented a state-of-the-art on the subject "Network Intrusion Detection for IoT Security based on Learning Techniques". In this scientific paper, the researchers presented a vision of the Internet of Things (architecture of IoT and threats against IoT). The researchers also presented a comparison of the open-source datasets used and a comparison of NIDS for IoT. They moreover presented Machine Learning algorithms and their use for NIDS for IoT. In 2019, Kelton A. P. da Costa et al [11] presented a state-of-the-art on the subject "Intrusion Detection Systems in Internet of Things Using Machine Learning". In this article, the authors presented the objective of each research work, the technique used, and the accuracy rate. Finally, they provided conclusions and a vision of the problems that existed in the works analyzed.

4. THE STATE OF THE ART

To improve the performance of IDSs, researchers in this field are starting to use artificial intelligence methods in the new work of IDS such as Artificial Neural Networks, Deep Learning, and Machine Learning which is our goal in this work. In what follows, we will present the recent work on IDSs in IoT based on the techniques of machine learning (Table 1).

In 2013, Monowar et al [12] presented a study on the detection of anomalies in the network, citing the known attacks against the networks, and the existing detection methods with a comparison between these methods. The authors also discussed the tools that could be used, the measures (criteria) test, and the set of data to use (datasets). Finally, this article provides some challenges to solve and some directions of research in this area.

In 2015, Mohuiddin Ahmed et al [13] presented a study on anomaly detection techniques in networks, and they divided these techniques into 4 categories, Classification, Statistical, Information Theory, and Clustering. The authors also explained the principles and techniques of each category and presented the datasets used in the domain and the limitations of each dataset. Finally, the authors proposed some directions of research to improve the performances of the IDSs such as the use of Data Mining and Machine Learning techniques.

Also in 2015, Kelton AP Costa et al [14] proposed a nature-inspired intrusion detection approach. The purpose of this approach is to estimate the pdf that is used in the OPFC algorithm-based data classification since the efficiency of clustering depends on the PDF estimate. After that, the authors tested their model on IDSs, comparing OPFC with the clustering of data based on k-means. Then, they tried to use meta-heuristic techniques to find the best value of k for the calculation of OPFC. According to the authors, the results obtained showed that the meta-heuristic methods and more precisely PA and PSO are better against the exhaustive research.

In another work in 2015, R. Singh et al [15] presented a technique based on OS-ELM for intrusion detection. This technique uses two

Table 1: Works on IDSs in IoT using MLA.

R	Year	Title	MLA	Accuracy
12	2013	Network Anomaly Detection: Methods, Systems and Tools	ADAM, SVM, CSF-KNN, OCSVM	-
13	2015	A survey of network anomaly detection techniques	SVM	-
14	2015	A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks	OPF, Bat, Firefly	-
15	2015	An intrusion detection system using network traffic profiling and online sequential extreme learning machine	OS-ELM	98.66%
16	2016	A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology	SVM	-
17	2016	Network Intrusion Detection Using Machine Learning Anomaly Detection Algorithms	k-means	80.19%
18	2016	An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization	SVM, MCLPDR	97.23%
19	2016	Random Forest Modeling for Network Intrusion Detection System	Random Forest	99.67%
20	2016	Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach	OPF clustering, SA-IDSs	96.02%
21	2016	Machine Learning Algorithms In Context Of Intrusion Detection	SVM, Naïve Bayes, J48	-
22	2017	An effective intrusion detection framework based on SVM with feature augmentation	SVM	99.18%
23	2017	A novel statistical technique for intrusion detection systems	LS-SVM	[99.62%-99.78]
24	2017	CLAPP: A self-constructing feature clustering approach for anomaly detection	KNN, SVM, J48	-
25	2017	Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT	Random Forest, Linear SVM, Multinomial	99.00% 92.00% 65.00%
26	2018	A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms	K-mean SVM	98.34%
27	2019	Internet of Things: A Survey on Machine Learning-based Intrusion Detection Approaches	-	-
28	2020	A Machine Learning Based Intrusion Detection System For Mobile Internet Of Things	Random Forest AMoF Linear Regression	DR : 90% - 98%
29	2020	Issues of Internet of Things (IoT) and an Intrusion Detection System for IoT Using Machine Learning Paradigm	Naïve Bayes	Precision : 96.8 %-94.7%
30	2020	Supervised Machine Learning Based Network Intrusion Detection System For Internet Of Things	Random Forest	Accuracy : 99.9% - 98.1%
31	2020	Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques	SVM Naïve Bayes Decision Tree AdaBoost	Accuracy : 98.95% 98.95% 97.89% 100%
32	2020	Intrusion Detection System In IoT Network Using Machine Learning	LS-SVM PSO	Accuracy : 92.69%-83.49%
33	2020	Improved Security Using Machine Learning For IoT Intrusion Detection System	-	Accuracy : 94.57%

34	2020	RDTIDS: Rules and Decision Tree-Based Intrusion Detection System For Internet Of Things Networks	REP Tree JRip Forest PA	Accuracy : 96.66% - 96.99%
35	2020	Botnet Attack Detection in Internet of Things Using Optimization Techniques	SVM, ANN, RF, GA	97,20%
36	2021	A Review of Intrusion Detection Systems in RPL Routing Protocol Based on Machine Learning for Internet of Things Applications	-	-
37	2021	Intrusion Detection System through Advanced Machine Learning for the Internet of Things Networks	SVM, Ensemble Classifier, DT	99.8%
38	2021	An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges	-	-
39	2021	Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset	Logistic Regression (LR), Naive Bayes (NB), k-Nearest Neighbor (kNN), Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), AdaBoost, XGBoost	97.80% - 98%
40	2021	Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks	JChaid∗ decision tree, A2DE Bayesian, Deep MLP, CNN, Unsupervised HGC	100%
41	2021	CoLL-IoT: A Collaborative Intruder Detection System for Internet of Things Devices	K-Nearest Neighbors (K-NN), Random Forest (RF), Extreme gradient boosting (XGBoost), Logistic Regression (LR)	98%
42	2022	Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets	-	-
43	2022	Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming	Support Vector Machine (SVM) Random Forest (RF) Linear Regression (LR)	98% 85% 78%
44	2022	XGB-RF: A Hybrid Machine Learning Approach for IoT Intrusion Detection	Random Forest (RF), Extreme Gradient Boosting (XGBoost)	99.94%
45	2022	Denial of service attack detection and mitigation for the Internet of Things using looking-back-enabled machine learning techniques	Long Short-Term Memory (LSTM), The Multi-Layer Perceptron (MLP), The K-Nearest Neighbors (KNN), Random Forest (RF), Decision Trees (DT)	99.81%
46	2023	Engineering the application of machine learning in an IDS based on IoT traffic flow	-	-
47	2023	Wrapper Based Linear Discriminant Analysis (LDA) for Intrusion Detection in IIoT	SVM, RF	97%
48	2023	Hybridized bio-inspired intrusion detection system for Internet of Things	KNN, XGBoost	84.75%
49	2023	Customized Intrusion Detection for an Industrial IoT Heterogeneous Network Based on Machine Learning Algorithms Called FTL-CID	-	85.52%
50	2023	Intrusion Detection Based on Bidirectional Long Short-Term Memory with Attention Mechanism	Bi-LSTM	99.05%

profiling parameters Alpha to reduce temporal complexity, and Beta to reduce the space of the training data set. NSL-KDD 2009 and Kyoto University are the two datasets used to evaluate the performance of the proposed work. According to the authors, the results obtained showed that the proposed method is effective in intrusion detection compared to other works.

In 2016, Hishem Sedjelmaci et al [16] developed a light technique for the detection of anomalies,

based on the concept of "Game Theory". Among the problems of IDSs in IoT devices is the power consumption when these IDSs are activated all the time. To solve this problem the authors used Game Theory with Nash Equilibrium with which the detectors of the anomalies are activated only when an attack foresees to occur. Finally, researchers said that their approach requires low energy consumption to detect attacks.

In another work in 2016, Khadija Hanafi et al [17] proposed a semi-supervised IDS based on the k-means algorithm. The idea of this proposed system is to divide the samples into 2 normal and abnormal categories during learning and then after distinguishing the samples according to their distance from the center of the cluster and calculating a threshold value. To evaluate their approach, the authors used the NSL-KDD dataset. According to the researchers, the implementation results of the proposed system gave an accuracy of 80.119%.

Also in 2016, Seyed Mojtaba Hosseini Bamakan et al [18] developed an intrusion detection framework based on an optimization called TVCPSO. The proposed approach is based on two classifiers MCLP and SVM. The main idea of this work is to apply the proposed TVCPSO method to define the parameters of the two classifiers and then propose a function that takes into account two metrics that are DR, FAR, and also the selection of characteristics.

Also In 2016, Nadia Farnaaz et al [19] proposed a model of IDS based on the machine learning algorithm Random Forest. The big tasks of this work are to use Random Forest for NIDS, classify the different types of attacks and improve the accuracy of this classifier in detecting different types of attacks. To evaluate the performance of this approach, researchers were using the NSL-KDD dataset and the following evaluation metrics: DR, FAR, and Accuracy.

In 2016, Hamid Bostani et al [20] developed a Hybrid Intrusion Detection Framework, which combines anomaly-based IDSs and specification-based IDSs using an unsupervised algorithm called OPF. Framework that is specifically designed for IoT networks. This framework works in real-time and its main purpose is to detect both Sinkhole and Selective Forwarding attacks. The part of this IDS is based on the specification installed in the router nodes and sends the results to the root, and the anomaly-based part installed in the root node. The latter uses the OPF algorithm to project clustering models using incoming data packets. The agent installed in the root is based on MapReduce architecture.

In 2016, Tahir Mahmood et al [21] presented a comparison between the different algorithms for supervised learning of machine learning for anomaly detection. This comparison uses the dataset KDD99, and the authors used the following metrics TPR, FPR and Accuracy to evaluate their work.

In 2017, H. Wang et al [22] proposed an intrusion detection framework based on the SVM algorithm with an increase in features. For the augmentation and formation of original features, the authors implemented LMDRT. To evaluate the performance of the proposed Framework, the researchers used the NSL-KDD dataset.

In 2017, Enamul Kabir et al [23] presented a new approach to intrusion detection based on sampling using the LS-SVM method. This approach is divided into two important steps, the first is to divide the dataset into certain predetermined subgroups to extract samples that are used in the second step of the approach, and this second step is to apply the LS-SVM method on the extracted data to detect intrusions. Researchers gave this approach the name OALS-SVM. To evaluate the performance of the proposed work, the KDD99 dataset is used.

In 2017, G. Rajesh Kumar et al [24] designed a fuzzy membership function to handle dimensionality and anomaly exploration to reduce the complexity of calculating and increasing accuracy. To evaluate their method, the authors used two DARPA and NSL-KDD datasets and three KNN, J48, and CANN algorithms, and they took as an example of attacks to detect both U2R and R2L attacks.

In 2017, Manuel Lopez-Martin and al [25] proposed a new method for intrusion detection for IoT networks. The proposed method is based on CVAE. According to the authors, this work is considered the first application of CVAE to increase the classification of intrusion data and also increase the reconstruction of characteristics. The results obtained showed that the proposed model is less complex than the other classifiers based on pure VAE.

In 2018, Nivaashini et al [26] proposed an IDS Framework for Internet of Things networks, more specifically for Wireless Sensor Networks (WSN). The researchers also proposed in this work the

construction of a new dataset from a WSN network. According to the authors, this dataset contains different types of attacks even those attacks that do not exist in the other datasets such as KDD Cup 99 database. The proposed IDS consists of three phases: the first is Dataset Collection, the second consists of Feature Extraction and the last contains Feature Selection and Attack detection. In the last phase, the researchers used two techniques: Clustering by K-mean algorithm and Classification by SVM algorithm. Finally, the results obtained by the researchers (Accuracy=98.34% and False Positive Rate=1.23%) showed that a Hybrid IDS is more efficient than an IDS with a single algorithm.

In 2019, Kelton A. P. da Costa et al [27] presented a study on Intrusion Detection Systems that are based on Machine Learning techniques to secure Internet of Things networks and applications. The researchers presented an analysis of more than 57 research works in the subject matter. Then, they gave a vision of the methods and datasets used. Finally, the authors have provided insights into the existing research challenges and problems for future research.

In 2020, Amouri et al [28] presented an IDS to secure IoT networks, precisely WSN and MANET networks. This IDS is a cross-layer based and it consists of two layers of detection. The first layer is dedicated to collecting the data and generating the CCIs using a Random Forest classifier, and the second layer is the super node (SN). At this level, the CCIs are sent to an algorithmically run super node that calculates quantities, which we refer to as AMoF. A linear regression process is then performed in parallel with the calculation of AMoF. For testing the proposed model, the researchers used both Blackhole and DDoS attacks, and this IDS is based on two Machine Learning algorithms which are Random Forest and Linear Regression.

In 2020, Mridha et al [29] began their article with a presentation of the different communication methods in IoT environments. Then, they presented a description of security, privacy, and interoperability issues in IoT networks. In the second part of this work, the authors proposed a real-time network intrusion detection system for the prediction of abnormal behavior of IoT networks and identifying compromised IoT devices on a network. According to the researchers, the proposed model consists of two stages. The first one consists of using Machine Learning to learn the normal behavior of an IoT network. This stage is divided into two phases. The first phase is dedicated to collecting data from the implemented network, whereas the second phase is dedicated to classifying the data into normal and abnormal data using Machine Learning. The second stage consists of rules configured and generated by the network administrator.

In 2020, Rani et al [30] proposed a NIDS based on supervised Machine Learning techniques, precisely the Random Forest algorithm. In this work, the authors used the two datasets KDD CUP 99 and NSL-KDD. These datasets contain 41 Features, but the researchers use only 10 Features for Testing and Training, and this reduction speeds up the operation of Training and increases the detection rate. Concerning the classification part, five classification tests are carried out, namely, Normal, DDoS, U2R, R2L, and Probe.

In 2020, Kirana et al [31] proposed an IDS based on Machine Learning techniques to detect Man-in-the-middle attacks in IoT networks. This proposed IDS contains 3 important phases: in the first phase a test is built to stimulate IoT environment (MCU ESP8266 node, DHT11 sensor, wireless router, think speak server) and the data captured from this environment are: temperature, humidity and points due). The second phase is the phase of building an attack system for attack testing. Normal and attack data must be generated from the environment prepared in the previous phase and the attack used is the Man-in-the-middle attack using Sniffing and ARP Poisoning. The third phase is to use Machine Learning algorithms to detect normal and attack data. The Machine Learning algorithms used are Naïve Bayes, SVM, Decision Tree and AdaBoost.

In 2020, Alrahman et al [32] presented an IDS based on Machine Learning techniques, precisely active learning to detect botnet attacks in IoT context. In this article, the work presented is based on supervised learning. The researchers used the LS-SVM algorithm as a classification technique, and they used the PSO algorithm for optimization. The proposed study aims to detect botnets in IoT networks. The main purpose of this article is to analyze how Active Machine Learning techniques work in IDS devices.

In 2020, Mandala et al [33] presented the security challenges for intrusion detection in IoT networks. Then they analyzed the different types of attacks against this type of network. Finally, the researchers were implementing a Machine Learning classification algorithm as part of intrusion detection to improve the rate of identifying attacks on IoT networks.

In 2020, Ferrag et al [34] proposed a hierarchical IDS, named RDTIDS, for IoT networks based on Machine Learning techniques. The idea that runs behind this article consists of using three classifiers that are based on two concepts: Decision Tree and Rules-Based. The first two classifiers, REP Tree and JRip, use the characteristics of the dataset and classify the traffic in Attack or Normal data. The third classifier, Forest algorithm (PA), takes as inputs the data characteristics and the outputs of the first and second classifiers.

In 2020, Rethinavalli et al [35] proposed an IDS based on optimization techniques for detecting Botnet attacks in IoT environments. The proposed intrusion detection in IDS is based on a Genetic Algorithm. To evaluate their work, the researchers compared their proposed method with machine learning algorithms such as SVM, ANN, and RF using KDD Cup as a dataset and Precision, Recall, F1 score and Area Under Curve (AUC) as evaluation parameters.

In 2021, Seyfollahi et al [36] presented a Review of Intrusion Detection Systems in RPL Protocol based on Machine Learning algorithms and techniques. First, the authors presented a Literature Review. Then, a study of the IDS in IoT and a study of the RPL protocol and attacks were presented. Besides, the researchers explained the methods of Machine Learning in the RPL protocol. Finally, they concluded their paper with a statistical analysis of the review and consequently by the challenges and research problems in the subject of intrusion detection in RPL protocol.

In 2021, Saba et al [37] proposed an Intrusion Detection System (IDS) Framework based on Machine Learning techniques for IoT network security. The proposed Framework is based on a hybrid method that contains two phases: in the first phase, the researchers used a Genetic Algorithm (GA) for feature selection, and in the second phase they used the algorithms of Machine Learning such as Support Vector Machine (SVM), Ensemble Classifier and Decision Tree. To test the proposed work, the researchers used the NSLKDD dataset.

In 2021, Adnan et al [38] presented a review on IDSs based on Machine Learning techniques for the security of the Internet of Things. The authors began their article with a general overview of IDSs and their approaches. Subsequently, they presented three challenges of IDSs, namely: The Concept drift, The High dimensional and The Computational Complexity. Following this, they presented the most widely recognized datasets in the context of Intrusion Detection. Finally, the authors summarized and discussed the challenges of IDSs for IoT.

In 2021, Gad et al [39] proposed an Intrusion Detection System using Machine Learning for the security of Vehicular Ad-Hoc Networks (VANETs). The proposed system has several components such as Data Pre-processing, Feature selection (with the Chi2 technique), Class balancing (with the SMOTE technique), Training ML Methods and Testing ML Methods. The parameters: Accuracy, Precision, Recall, F1-score and False FPR are calculated by the researchers based on ToN-IoT dataset to evaluate the proposed system.

In 2021, Panda et al [40] proposed a Feature Engineering and Machine Learning model for detecting IoT-Botnet attacks. The proposed model is a combination of K-Mediod Sampling and Scatter Search-based Feature Engineering on one side and Machine Learning (JChaid, A2DE, and HGC) and Deep Learning (DMLP, CNN) on the other. To test their model, researchers took Accuracy, Precision, Recall and F1-score as evaluation parameters and UNSW-NB15 as a dataset.

In 2021, Alshahrani et al [41] presented a Collaborative Intrusion Detection System called CoLL-IoT for IoT devices. The researchers divided the proposed system into four layers: IoT layer, Network layer, Fog layer and Cloud layer. These layers monitor and collaboratively analyze network traffic to detect intrusions. To increase the detection performance of the proposed system, the authors used the algorithms of Machine Learning including K-Nearest Neighbors (K-NN), Logistic Regression (LR), Random Forest (RF) and Extreme Gradient Boosting (XGBoosting). CoLL-IoT was evaluated on UNSW-NB15 dataset based on 4 evaluation parameters which are: Accuracy, FPR, FNR and F1-Score.

In 2022, Gyamfi et al [42] presented a review of Network Intrusion Detection Systems (NIDS) for IoT networks. This Review contains an analysis of the approaches based on Multi-Access Edge Computing (MEC) and utilizing machine learning techniques. The researchers performed a comparative study of the most widely used public datasets in the field of IoT safety, and they also presented assessment metrics for IoT-based NIDS. Finally, they proposed a model of a Network Intrusion Detection System (NIDS) for IoT Systems.

In 2022, Raghuvanshi et al [43] proposed an Intrusion Detection System Framework for IoT

networks, and more specifically for Smart Farming. This Framework can be divided into two phases: the first phase is known as data Pre-processing from the NSL-KDD dataset, and the second phase is responsible for data classification. In this phase, the researchers used Machine Learning algorithms such as Support Vector Machine (SVM), Linear Regression (LR), and Random Forest (RF) focusing on three evaluation parameters which are Accuracy, Precision and Recall.

In 2022, Al Faysal et al [44] proposed a diagram of an Intrusion Detection System for IoT networks. The proposed hybrid scheme contains two parts: the first part is the selection of features using the Random Forest (RF) algorithm, and the second part is the classification which is based on the Extreme Gradient Boosting technique (XGB). To test their proposed model, the researchers applied this model to the N-BaIoT dataset using the following evaluation parameters: accuracy (ACC), F1 score, Kappa index, Matthew's correlation coefficient (MCC), sensitivity (SE), specificity (SP), Threat Score, balanced accuracy.

In 2022, Mihoub et al [45] proposed an Intrusion Detection System architecture to detect DoS/DDoS attacks in IoT networks. The proposed architecture is composed of two components: detection and mitigation. The detection component is a multi-class classifier that adopts the "Looking Back" concept. The researchers used several Machine Learning models such as Decision Table (DT), Random Forest (RF), K-Nearest Neighbors (KNN), Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM). These models are tested on the Bot-IoT dataset based on the following evaluation parameters: Accuracy and Kappa Index.

In 2023, Prazeres et al [46] proposed an Intrusion Detection System based on Fog Computing with a distributed architecture to identify and detect malicious data inside IoT-Flow. The proposed model consists of three phases: Pre-processing and feature selection which are applied to the generated IoT-Flow and the last phase is classification with Deep Neural Networks.

In 2023, Yasotha et al [47] proposed a training process and a wrapper-based feature selection for IDS to present a security solution for IoT. The feature selection is based on a wrapper with Direct Linear Discriminant Analysis (WDLDA). The architecture of the work proposed by the researchers is divided into four phases: Pre-processing, Feature selection, Classification and finally processing. The authors used the NSL-KDD dataset to test their proposal.

In 2023, Singh et al [48] proposed a bio-inspired Hybrid Intrusion Detection System to secure the Internet of Things. According to the researchers, the proposed work is divided into two major phases, the first phase is the Feature Selection phase where the researchers used two algorithms: the Sinus-Cosinus algorithm (SCA) and the Salp Swarm algorithm (SSA). The second phase is the classification phase where the researchers used two Machine Learning classifiers KNN and XGBoost.

In 2023, Abosata et al [49] presented a Distributed Intrusion Detection System named (FT-CID) to detect RPL intrusion in Internet of Things. The proposed model includes three phases: dataset collection, IDS learning based on FTL, and intrusion detection.

In 2023, Yang et al [50] presented an intrusion detection model based on Bidirectional Long Short-Term Memory with Attention Mechanism. The proposed model is divided into 3 parts: Pre-processing, categorization with Bi-LSTM and Attention Mechanism and the last part consists of collecting the data generated by the IoT clusters. To test the proposed model, the researchers used the UNSW-NB15 dataset and the three evaluation parameters: Accuracy, Detection Rate, and F1-Score.

5. ANALYSIS AND DISCUSSION

5.1 Analysis

The research works presented in our state-of-the-art are extracted from confirmed databases such as IEEE Xplore, Springer, and Science Direct … Etc. Figure 3 below shows the number of articles considered in this work on each database.

In this state of the art, we studied and analyzed 34 articles, these articles were published between 2013 and 2023 in journals indexed in confirmed databases. Figure 4 shows the number of articles considered in each year from 2013 to 2023.

Several datasets have been used by researchers to propose and test IDS solutions based on machine learning techniques to secure IoT. Some works are based on well-known datasets in the field of IDSs such as NSL-KDD, on the other hand, other works are based on datasets created locally, and other works are based on a collection of datasets. In the following, we will present Figure 5 that shows the number of times each dataset is used.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Researchers in the Internet of Things security field with Machine Learning algorithms are still trying to find the Machine Learning algorithm that can work well. Figure 6 below reveals the Machine Learning techniques most used by researchers to propose IDS solutions to secure networks and Internet of Things applications:

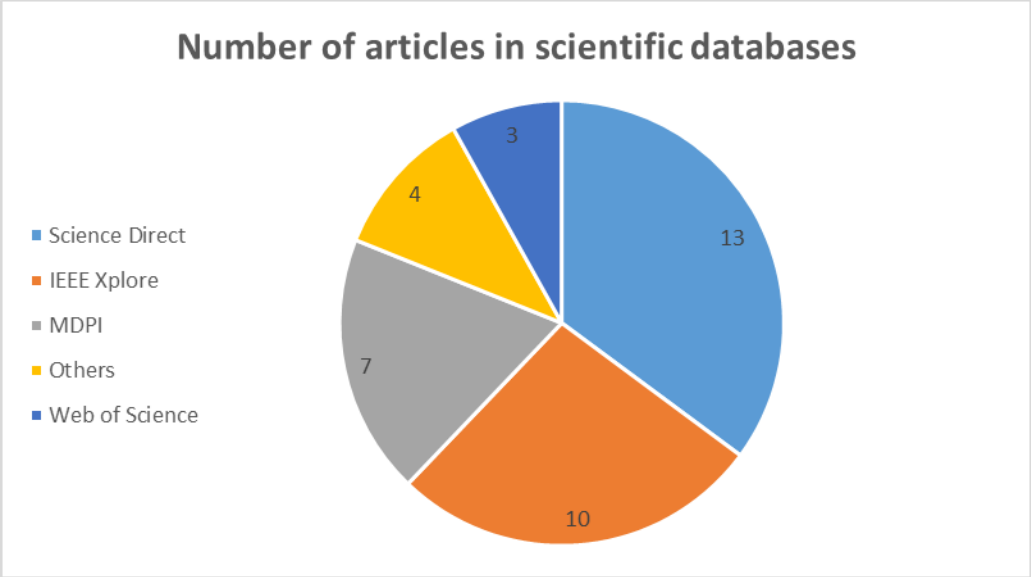

Figure 3: Number of articles in scientific databases

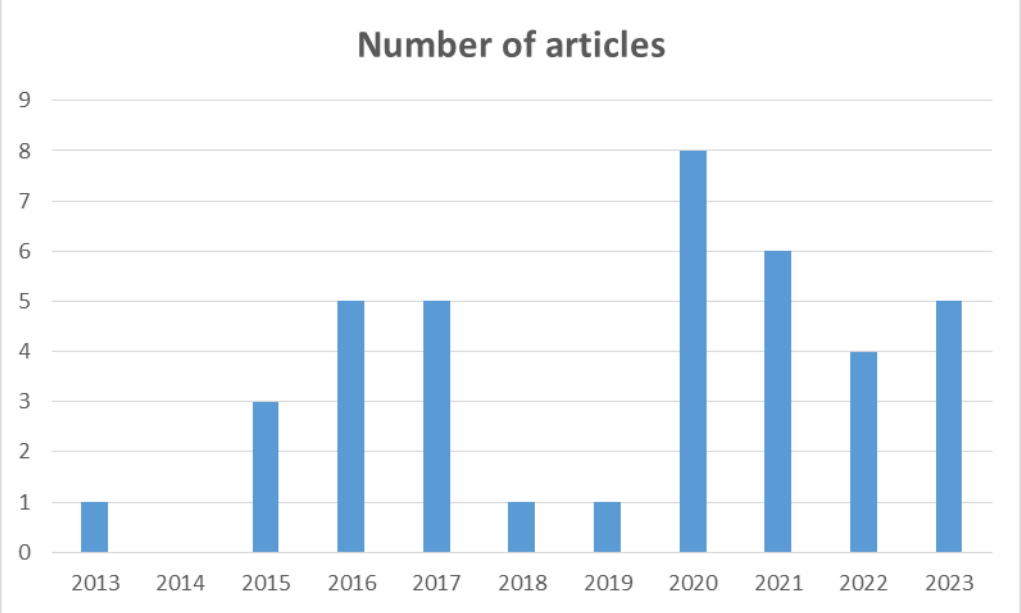

Figure 4: Number of articles

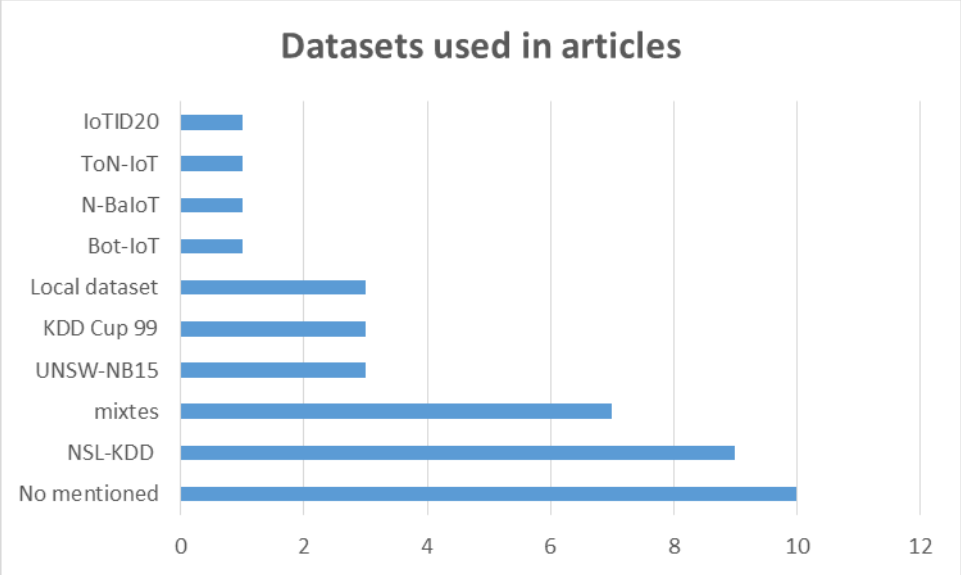

Figure 5: Datasets used in articles

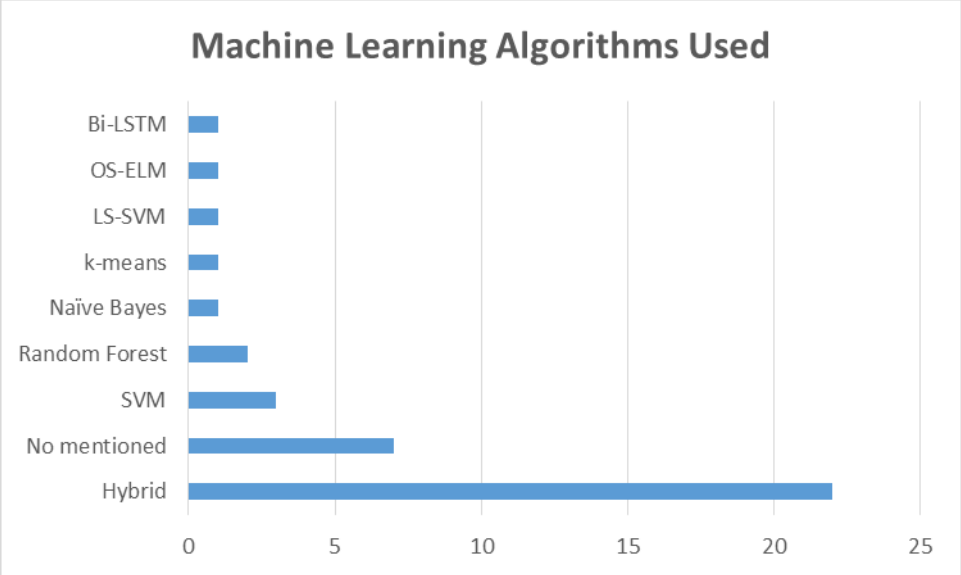

Figure 6: Machine Learning Algorithms used

5.2 Discussion

The main objective of our work is to present the state of advancement on the use of IDSs based on machine learning techniques for IoT security. To achieve this goal, we presented in the previous subsection a statistical and analytical study of the collected research works. According to this detailed analytical study, it was first noted that since 2020 the number of articles published on the theme "Intrusion Detection Systems for environments IoT based on machine learning techniques" has increased. This can be interpreted as the increasing use of machine learning as a solution to enhance the accuracy of IDSs in IoT networks. On the other hand, we see that the widely used datasets in the analyzed articles are NSL-KDD, KDD Cup 99, and UNSW-NB15. This is due to data consistency, the features used, and the existing attacks. Finally, concerning the algorithms and techniques of Machine Learning used, we conclude that SVM, Random Forest, Naive Bayes, and K-means are often used but the commonly adopted idea by

researchers on the side of the chosen algorithms is the idea of mixing, that is to say of offering hybrid solutions. In what follows, we will discuss the role, advantages, and disadvantages of each of the Machine Learning algorithms most frequently presented in Figure 6:

Firstly, Support Vector Machine (SVM): It is one of the supervised learning algorithms. SVM is widely used for classification, and its principle is to separate data into different classes. This algorithm works accurately when there is a clear margin of separation between classes and in the case where the number of dimensions exceeds the number of samples. On the other hand, this algorithm has some disadvantages, such as the inability to suit large data and large processing time in classification. Secondly, Random Forest: It is a supervised learning algorithm, used for classification and regression problems. The basic idea of this algorithm is to build several decision trees in the training time and each tree makes a prediction and the result is Average for Regression and Majority votes for classification. Among the strong points of this algorithm, we have flexibility and robustness because it manages all types of data and missing values, and it is characterized by parallel processing thanks to the concept of trees. On the opposite side, this algorithm requires a large volume of memory especially in the case of large datasets, and is less interpretable due to the large number of trees. Thirdly, Naive Bayes: It is a supervised learning algorithm intended to solve classification problems. This algorithm is based on Bayes' probability theorem with independence between features. The advantages of Naive Bayes algorithm are summarized in its simplicity, ease of use, and not requiring a large volume of data for training phase. On the disadvantage side, we find that Naive Bayes can find difficulties with imbalanced datasets, and it assumes that all features are independent which is not always possible. Finally, K-means: It is an unsupervised learning algorithm that is used in Clustering problems. The role of K-means is to group similar data based on distance and similarity and difference between data points. This algorithm is recognized for its flexibility, simplicity, and its management of large datasets. On the other hand, it suffers from sensitivity to outliers and dependence on the initialization of clusters.

In the works we have analyzed, various techniques, methodologies, and models are used to present solid IDS solutions based on machine learning to effectively secure IoT networks. Through the differentiation of the presented works, it was observed that there is a divergence in perspectives in the literature that we have prepared in this article. This differentiation is due to several factors, including firstly, the targeted network type. Each type of IoT network has its special structure and characteristics. For example, the characteristics of WSNs are not the same as those of MANETs. Secondly, the dataset used, we know that the starting point in Machine Learning-based solutions is the dataset used. In this context, we found that researchers use different datasets with varying numbers of features. Thirdly, the factor of targeted attacks, in other words, each type of attack or each attack has a detection strategy. Fourthly, the techniques and models used, each research work aims to find a method or model that can yield good results. In the works we have analyzed, we found several interesting methods, such as Nature-Inspired approach, Game-Theoric methodology, Active Learning, etc. Finally, the most important factor from our perspective is the algorithm used because we have observed that in each research work, researchers strive to select the most adaptable algorithm for the proposed model. In several cases, researchers modify the algorithm to discover a more efficient variant, and in other instances, researchers work with multiple algorithms to find a more effective hybrid solution in intrusion detection. All these factors provide us with contradictory perspectives in the works presented in this paper.

Despite the efforts put forth by researchers to provide different solutions compatible with the IoT infrastructure, there remains a significant deficiency of distributed artificial intelligence techniques and multi-agent systems.

In the context of analyzing research on the integration of Machine Learning techniques into IDSs to enhance the security of the Internet of Things, several works have been published in recent years [10] [11]. Comparing our work with the other publications, we find that in [10], the researchers presented a good study, yet they were limited to studying a single type of IDS which is the Network Intrusion Detection System. On the other hand, in another work in [11], the authors presented a study on Machine Learning approaches in IDSs for the security of Internet of Things. The drawbacks of this study lie in the absence of statistical and analytical aspects of the examined work, the lack of analysis and discussion of Machine learning algorithms, and the deficiency in the details of the presented summaries of the collected articles. This motivates us to present our work, in the form of a state-of-the-art, analytical and statistical study, and

consequently, an advancement in the treatment of the theme "Intrusion Detection systems based on Machine Learning Techniques for Internet of Things Security."

Our work can be considered as an update and development of previous similar studies [10] [11]. Firstly, our work includes most of the scientific articles published on the treated subject between 2013 and 2023. Secondly, it provides a detailed description of all the collected research. Thirdly, it presents a statistical and analytical study of the collected works. Finally, we have presented the most commonly used Machine Learning algorithms with a discussion of their advantages and disadvantages.

6. CONCLUSION AND FUTURE WORK

Machine learning is considered one of the most widely used artificial intelligence techniques in the field of securing Internet of Things networks. In this scientific paper, we presented the advancement in the field of using Intrusion Detection Systems based on machine learning to secure Internet of Things networks by reviewing the state of the art and analyzing most of the research published in this regard between 2013 and 2023. Moreover, we provided an analytical and statistical study of the research topic. The importance and impact of our work lies in providing the scientific community with a comprehensive and detailed insight into the machine learning techniques and algorithms used in constructing intrusion detection systems to secure Internet of Things. Our future work will focus on providing a solution for intrusion detection systems based on distributed artificial intelligence and multi-agent systems and how to integrate these technologies into intrusion detection systems to provide effective security solutions for Internet of Things, and we are currently engaged in progressing in this research.

REFERENCES:

[1] Sade Kuyoro, Folasade Osisanwo, Omoyele Akinsowon, "Internet of Things (IoT): An Overview", Proceedings of the 3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015), IEEE Explore, March 23-24, pp. 53-58.

[2] Parvaneh Asghari, Amir Masoud Rahmani, Hamid Haj Seyyed Javadi, "Internet of Things applications: A systematic review", Computer Networks, 148 (2019), 2019, pp. 241–261.

[3] Fadele Ayotunde Alabaa, Mazliza Othmana, Ibrahim Abaker Targio Hashema, Faiz Alotaibib, "Internet of Things security: A survey", Journal of Network and Computer Applications, 88(2017), 2017, pp. 10-28.

[4] https://www.oracle.com/fr/internet-of-things/what-is-iot/ (07/12/2023)

[5] https://iotdunia.com/iot-architecture/ (07/12/2023)

[6] Hongyu Liu, Bo Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey", Applied Sciences, Volume 9, Issue 20, 2019, pp. 1-28.

[7] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah and Farhan Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Transactions on Emerging Telecommunications Technologies, Volume 32, Issue 1, 2021, pp. 1-29.

[8] Proko, Eljona, Alketa Hyso, Dezdemona Gjylapi, "Machine Learning Algorithms in Cyber Security", Proceedings of the 3rd International Conference on Recent Trends and Applications in Computer Science and Information Technology (RTA-CSIT 2018), CEUR Workshop Proceedings, Nov 23-24, 2018, pp. 203-207.

[9] Aized Amin Soofi, Arshad Awanw, "Classification Techniques in Machine Learning: Applications and Issues", Journal of Basic & Applied Sciences, 13(2017), 2017, pp. 459-465.

[10] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, Parvez Faruki, "Network Intrusion Detection for IoT Security based on Learning Techniques", IEEE Communications Surveys & Tutorials, Volume 21, Issue 3, 2018, pp. 2671-2701.

[11] Kelton A.P. da Costaa, João P. Papaa, Celso O. Lisboaa, Roberto Munoz, Victor Hugo C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches", Computer Networks, 151(2019), 2019, pp. 147-157.

[12] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, Volume 16, Issue 1, 2013, pp. 303-336.

[13] Mohiuddin Ahmed, Abdun Naser Mahmoud, Jiankun Hu, "A survey of network anomaly detection techniques", Journal of Network and Computer Applications, 60(2016), 2016, pp. 19-31.

[14] Kelton A.P. Costa, Luis A.M. Pereira, Rodrigo Y.M Nakamura, Clayton Pereira, Joao P. Papa, and Alexandre Xavier Falcao, "A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks ", Information Sciences, 294(2015), 2015, pp. 95-108.

[15] Raman Singh, Harish Kumar, R.K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine", Expert Systems with Applications, Volume 42, Issue 22, pp. 8609-8624.

[16] Hichem Sedjelmaci, Sidi Mohammed Senouci, Mohamad Al-Bahri, "A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology ", Proceedings of the IEEE International Conference on Communications (ICC), IEEE Xplore, May 22-27, 2016, pp. 1-6.

[17] Khadija HANIFI and Hasan BANK. 2016. Network Intrusion Detection Using Machine Learning Anomaly Detection Algorithms. Proceedings of the 25th Signal Processing and Communications Applications Conference, May 15-18, IEEE Xplore, pp: 1-4.

[18] Seyed Mojtaba Hosseini Bamakan, Haudong Wang, Tian Yingjie, Yong Shi, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization ", Neurocomputing, 199(2016), 2016, pp. 90-102.

[19] Nabila Farnaaz and M. A. Jabbar, "Random Forest Modeling for Network Intrusion Detection System ", Procedia Computer Science, 89(2016), 2016, pp. 213-217.

[20] Hamid Bostani and Mansour Sheikhan, "Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach", Computer Communications, 98(2017), 2017, pp. 52-71.

[21] Tahir Mehmood, Helmi B Md Rais, "Machine Learning Algorithms In Context Of Intrusion Detection", Proceedings of the 3rd International Conference on Computer and Information Sciences (ICCOINS), IEEE Xplore, August 15-17, 2016, pp. 369-373.

[22] Huiwen Wang, Jie Gu, Shanshan Wang, "An effective intrusion detection framework based on SVM with feature augmentation", Knowledge-Based Systems, 136(2017), 2017, pp. 130-139.

[23] Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo, "A novel statistical technique for intrusion detection systems", Future Generation Computer Systems, 79(2018), 2018, pp. 303-318.

[24] Gunupudi Rajesh Kumar, Nimmala Mangathayaru, Gugulothu Narsimha, Gali Suresh Reddy, "CLAPP: A self-constructing feature clustering approach for anomaly detection", Future Generation Computer Systems, 74(2017), 2017, pp. 417-429.

[25] Manuel Lopez-Martin, Belen Carro, Antonio Sanchez-Esguevillas, Jaime Lloret, "Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT". Sensors, Volume 17, Issue 9, 2017, pp. 1-17.

[26] Nivaashini M and Thangaraj P, "A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms", Proceedings of the International Conference on Computing, Power and Communication Technologies (GUCON), IEEE Xplore, Sept 28-29, 2018, pp. 44-49.

[27] Kelton A.P. da Costa, Joao P. Papa, Celso O. Lisboa, Roberto Munoz, Victor Hugo C. de Albuquerque, "Internet of Things: A Survey on Machine Learning-based Intrusion Detection Approaches", Computer Networks, 151(2019), 2019, pp. 147-157.

[28] Amar Amouri, Vishwa T. Alaparthy, Salvatore D. Morgera, "A Machine Learning Based Intrusion Detection System For Mobile Internet Of Things" Sensors, Volume 20, Issue 2, 2020, pp. 461. 1-15.

[29] M.F. Mridha, Md. Abdul Hamid, Md. Asaduzzaman, "Issues of Internet Of Things (IoT) and an Intrusion Detection System for IoT Using Machine Learning Paradigm", Proceedings of the International Joint Conference on Computational Intelligence, SpringerLink, Dec. 14-15, 2020, pp. 395–406.

[30] Deepa Rani, Dr. Narottam Chand Kaushal, "Supervised Machine Learning Based Network Intrusion Detection System For Internet Of Things", Proceedings of the 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE Xplore, Jul 01-03, 2020, pp. 1-7.

[31] K. V. V. N. L Sai Kirana, R. N. Kamakshi Devisettya, N. Pavan Kalyana, K. Mukundinia, R. Karthia, "Building a Intrusion Detection System for IoT Environment using Machine

Learning Techniques", Procedia Computer Science, 171(2020), 2020, pp. 2372-2379.

[32] Abdulrahman Salim A.Alrahman, Dr. Abdullahi Abdu Ibrahim, "Intrusion Detection System In IoT Network Using Machine Learning", Proceedings of the 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE Xplore, Oct. 22-24, 2020, pp. 1-5.

[33] K.Mandala, M.Rajkumara, P.Ezhumalaia, D.Jayakumara, R.Yuvaranib, "Improved Security Using Machine Learning For IoT Intrusion Detection System", Proceedings of the International Conference on Emerging Trends in Materials Science, Technology and Engineering (ICMSTE2K21), Science Direct, 2020, pp. 1-5.

[34] Mohamed Amine Ferrag, Leandros Maglaras, Ahmed Ahmim, Makhlouf Derdour, Helge Janicke, "RDTIDS: Rules and Decision Tree-Based Intrusion Detection System For Internet Of Things Networks", Future Internet, Volume 12, Issue 3, 2020, pp. 1-14.

[35] Dr. S. Rethinavalli, Dr. R. Gopinath, "Botnet Attack Detection in Internet of Things Using Optimization Techniques", International Journal of Electrical Engineering and Technology (IJEET), Volume 11, Issue 10, 2020, pp. 412-420.

[36] Ali Seyfollahi, Ali Ghaffari, "A Review of Intrusion Detection Systems in RPL Routing Protocol Based on Machine Learning for Internet of Things Applications", Wireless Communications and Mobile Computing, 2021, pp. 1-32.

[37] Tanzila Saba, Tariq Sadad, Amjad Rehman, Zahid Mehmood, Qaisar Javaid, "Intrusion Detection System through Advance Machine Learning for the Internet of Things Networks", IEEE Xplore, IT Professional, Volume 23, Issue 2, 2021, pp. 58-64.

[38] Ahmed Adnan, Abdullah Muhammed, Abdul Azim Abd Ghani, Azizol Abdullah, Fahrul Hakim, "An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges", Volume 13, Issue 6, 2021, pp. 1-13.

[39] Abdallah R. Gad, Ahmed A. Nashat, Tamer M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset", IEEE Access, 9(2022), 2022, pp. 142206-142217.

[40] Mrutyunjaya Panda, Abd Allah A. Mousa, Aboul Ella Hassanein, "Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks", IEEE Access, 9(2021), 2021, pp. 91038-91052.

[41] Hani Mohammed Alshahrani, "CoLL-IoT: A Collaborative Intruder Detection System for Internet of Things Devices", Electronics, Volume 10, Issue 7, 2021, pp. 1-19.

[42] Eric Gyamfi and Anca Jurcut, "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets", Sensors, Volume 22, Issue 10, 2022, pp. 1-33.

[43] Abhishek Raghuvanshi, Umesh Kumar Singh, Guna Sekhar Sajja, Harikumar Pallathadka, Evans Asenso, Mustafa Kamal, Abha Singh, Khongdet Phasinam, "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming", Journal of Food Quality, 2022, pp. 1-8.

[44] Jabed Al Faysal, Sk Tahmid Mostafa, Jannatul Sultana Tamanna, Khondoker Mirazul Mumenin, Md. Mashrur Arifin, Md. Abdul Awal , Atanu Shome, Sheikh Shanawaz Mostafa, "XGB-RF: A Hybrid Machine Learning Approach for IoT Intrusion Detection", Telecom, Volume 3, Issue 1, 2022, pp. 52-69.

[45] Alaeddine Mihoub, Ouissem Ben Fredj, Omar Cheikhrouhou, Abdelouahid Derhab, Moez Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques", Computers & Electrical Engineering, 98(2022), 2022, pp. 107716.

[46] Nuno Prazeres, Rogério Luís de C. Costa, Leonel Santos, Carlos Rabadão, "Engineering the application of machine learning in an IDS based on IoT traffic flow", Intelligent Systems with Applications, 17(2023), 2023, pp. 200189.

[47] B. Yasotha, T. Sasikala and M. Krishnamurthy, "Wrapper Based Linear Discriminant Analysis (LDA) for Intrusion Detection in IIoT", Computer Systems Science and Engineering, Volume 45, Issue 2, 2023, pp. 1625-1640.

[48] Richa Singh, R. L. Ujjwal, "Hybridized bio-inspired intrusion detection system for Internet of Things", Front, Big Data 6, 2023, pp. 1081466.

[49] Nasr Abosata, Saba Al-Rubaye and Gokhan Inalhan, "Customised Intrusion Detection for an Industrial IoT Heterogeneous Network Based on Machine Learning Algorithms Called FTLCID", Sensors, Volume 23, Issue 1, 2023, pp. 1-20.

[50] Yongjie Yang, Shanshan Tu, Raja Hashim Ali, Hisham Alasmary, Muhammad Waqas, Muhammad Nouman Amjad, "Intrusion Detection Based on Bidirectional Long Short-Term Memory with Attention Mechanism", CMC-Computer Material and Continua, Volume 74, Issue 1, 2023, pp. 801-815.