

# An overview of machine and deep learning-based intrusion detection systems in the Internet of Things

Oumeima Boubertakh<sup>1</sup>, Ramdane Maamri<sup>1</sup> and Ali Sahnoun<sup>1</sup>

<sup>1</sup>LIRE Laboratory, University of Constantine 2 Abdelhamid Mehri

## Abstract

The Internet of Things (IoT) is one of the hottest topics in the industrial and academic fields in recent years, and it is regarded as the next revolution of the internet. IoT security and privacy issues have proven to be critical targets. Since IoT devices have less memory, processing power, and power consumption, traditional security mechanisms are ineffective. Thus, A security mechanism called an Intrusion Detection System (IDS) has an important role in securing IoT nodes and networks. Machine learning and deep learning techniques have been proposed for automatic intrusion detection and abnormal behavior identification of networks. Hence, in this filed, the types of IDS, the recent research, and contributions to IDS in IoT networks are discussed in this paper.

## Keywords

Internet of Things, Intrusion Detection Systems, Machine Learning, Deep Learning

## 1. Introduction

The Internet of Things (IoT) is one of the most rapidly evolving technological trends in recent years. According to [1] the number of IoT devices will reach 75 billion by 2025. Moreover, IoT is a new technology that collects data from the physical world and then transmits it over the internet to be exchanged, processed, and stored. By using actuators and smart appliances, the collected data is used to extract information and act on the physical world [2]. Moreover, IoT has noticeably increased human day activities such as the delivery of efficient healthcare services and the development of smart cities, homes and intelligent transportation systems [3]. Because of the resource limitations of the IoT, and the explosion in the number of unsecured IoT devices connected to the global network, IoT devices are more vulnerable and can be easily exploited by an attacker. Hence, the demands of IoT security is paramount. According to the literature, many works provide security in the IoT by utilizing cryptography based security mechanisms such as symmetric key cryptosystems and public key cryptosystems. Furthermore, cryptographic security mechanisms are primarily used to detect external attacks such as eavesdropping and message alteration. When the encryption methods hold the valid key and are compromised by the attack, they are unable to detect the vulnerable nodes. Attackers can easily obtain security details from compromised nodes and launch a series of internal intrusions [4]. As a result, the IDS serves as a tool to provide an additional level of security to the IoT.


---

RIF'23: The 12th Seminary of Computer Science Research at Feminine, March 09, 2023, Constantine, Algeria

✉ [oumeima.boubertakh@univ-constantine2.dz](mailto:oumeima.boubertakh@univ-constantine2.dz) (O. Boubertakh); [ramdane.maamri@univ-constantine2.dz](mailto:ramdane.maamri@univ-constantine2.dz) (R. Maamri); [ali.sahnoun@univ-constantine2.dz](mailto:ali.sahnoun@univ-constantine2.dz) (A. Sahnoun)



© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

Machine Learning (ML) and Deep Learning (DL) techniques have recently been developed and applied for intrusion detection and identification of abnormal behaviors in networks and their prevention.

The remainder of the paper is structured as follows: In Section 2, we present IoT security challenges that face the implementation of security policies, while in Section 3, IoT security goals are discussed. In Section 4, we offered a classification of IDS destined for the IoT. While in Section 5, a discussion of ML and DL for IDS is presented. Section 6 discusses metrics for evaluating the effectiveness of intrusion detection systems (IDSs). Section 7 presents the relevant work on various existing IDSs using ML and DL techniques. Section 8, a discussion of IDS-related works, is presented. The final section provides a conclusion and some future work directions.

## 2. IoT security challenges

IoT is an evolutionary technology that has gained enormous traction in science and engineering applications for solving problems without the intervention of human-machine physical contact. The advancement of internet technologies has enabled the possibility of wider and stronger network connectivity between the objects. Every object in IoT is identified as a node and is connected to each other in a network, allowing information sharing such as receiving and sending[5]. Because these devices operate in an Internet-connected environment, they are susceptible to various vulnerabilities and attacks[2]. As a result, IoT security must be addressed; however, there are numerous challenges in the IoT domain that complicate the development of security solutions, including the following:

- All "things" will be able to communicate with each other. As a result, there are numerous access points that can be used to exploit existing vulnerabilities[6].
- IoT devices typically have limited resources such as low processing power, limited energy, and limited memory. as a result, complex security algorithms may not be supported. [6]. Furthermore, the majority of devices lack the necessary hardware and software to support TCP/IP and security protocols[7].
- IoT devices are easily damaged, stolen, and compromised because they are everywhere[7].
- Heterogeneity of devices and network technologies: The IoT employs a wide range of sensors, devices, and network technologies, which can lead to a variety of security issues. It also makes the development of strong security policies more difficult[7].
- Lack of standardization: There are no unique standards that all IoT device builders use. Each vendor has his or her own set of standards, protocols, and technologies[7].

## 3. Why IoT protection is necessary

Security principles are essential in IoT for achieving reliable communications between devices, software, and people. Raising concerns that IoT is rapidly evolving without paying attention to the regulatory changes and significant security challenges that may be required. The most important concern in adopting IoT technology is security. This section will focus on the three

IoT security goals known as the CIA triad (confidentiality, integrity, and availability).Show Figure1.

1. Confidentiality: It is a security feature that means only the sender and receiver can read the information as it travels through the network[7].
2. Integrity: It must be ensured that the data or message was not altered or destroyed during its exchange, transmission, storage, and processing[8].
3. Availability: The process of ensuring availability is defined as making the required service (or a device) available anywhere and at any time for the intended users.[9].

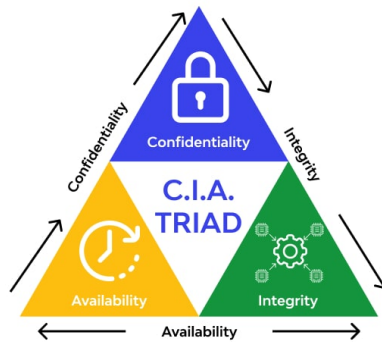


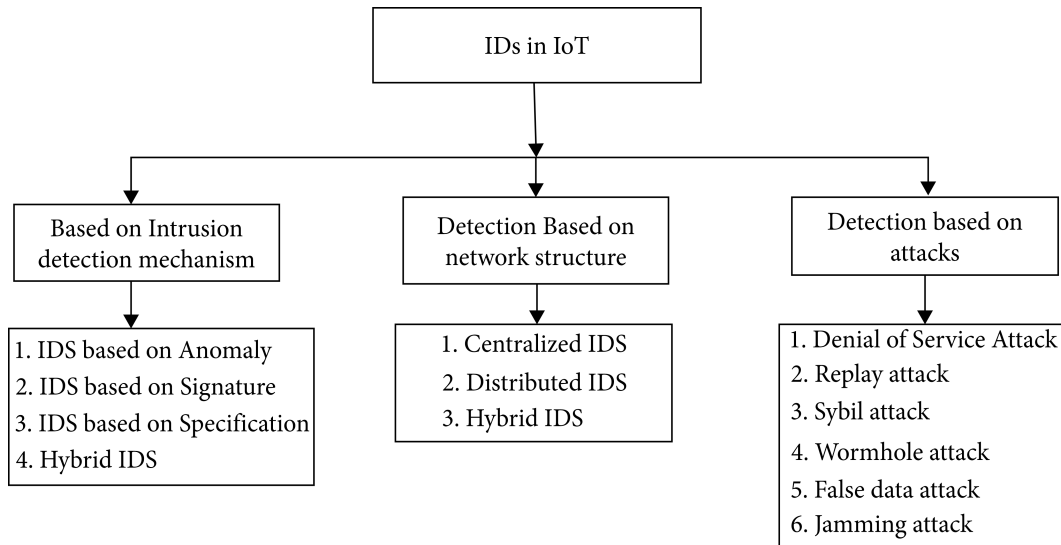
Figure 1: CIA TRIAD[10]

#### 4. Intrusion Detection System Taxonomy for IoT

Reference[11],defines an IoT intrusion as a disallowed operation or activity that endangers the IoT environment,In other words,any attack that compromises the confidentiality, integrity, or availability of information is classed as an intrusion. Intrusion detection is the process of monitoring and analyzing network traffic in order to detect malicious attacks (also known as intrusions) and respond to them with signs of intrusion[12].

The purpose of IDS is to identify different types of harmful network traffic and computer activities that a regular firewall might miss.The firewall can only detect attacks from outside the network,while IDSs are widely used to identify known and unknown network attacks from internal and external attackers[13],they serve as the last line of defense and are capable of determining the legitimacy of actions taken as well as acting pro-actively in attack situations[14].This is critical for obtaining high levels of security against acts that jeopardize IoT systems' availability, integrity, or secrecy.

According to [3], IDS in the IoT are classified into three types: those based on the intrusion detection mechanism, those based on network structure, and those developed by focusing on attack types.Show Figure2.



**Figure 2:** Taxonomy of IDS for IoT[3]

#### 4.1. IDS-based mechanism

IDS-based mechanism is further classified into four groups, anomaly detection, signature detection, specification and hybrid IDS

1. **IDS Based on Anomaly Detection:** This technique compared the behaviour of the devices with their normal behaviour. To detect the intrusion, a threshold value is used to determine whether a device's deviation exceeds the threshold. Such a device will be categorized as a suspect device and will be monitored over time. If a device's abnormal behaviour persists, it will be classified as malicious and isolated from communication with other devices[3].
2. **IDS Based on Signature:** This kind of IDS necessitates a database where all possible known attack patterns are stored and is extremely effective against known attacks. Moreover, it requires periodic updates because the system's efficiency is dependent on attack signatures stored in the database[3, 4].
3. **Specification-Based IDS:** These IDSs include a rule-set and some thresholds that go with it, Moreover, experts define these rules regarding the normal and abnormal activities of network nodes and protocols. whenever there is a deviation from the specified THs and rules. It is regarded as an attack. similar to anomaly-based IDS. in specification based-IDS the rules and thresholds are set by the human experts, but in anomaly-based IDS, the system should be trained[4].
4. **Hybrid IDS:** Hybrid IDSs are created by combining one or more of the previously mentioned IDS types. These IDSs are designed to improve performance by minimizing drawbacks and maximizing benefits. The detection accuracy and performance of the hybrid IDS are improved by combining the benefits of such IDSs[4].

## 4.2. IDS based on network structure

The IDS detection based on network structure is further classified into centralised IDS , distributed IDS , and hybrid IDS

1. Centralized IDS (CIDS): In this strategy, IDS are installed on a centralized router or a dedicated server, where they analyze the data available in network traffic and control all of the network's devices to detect intrusions[3].
2. Distributed IDS (DIDS): In this method, IDSs are installed on sensing nodes in IoT devices. Thus, each node in the IoT network is responsible for monitoring and identifying the behaviour of IoT device nodes in order to detect intrusions. Moreover, the resource-constrained properties of the IoT in this strategy should be examined and optimized[3][4].
3. Hybrid IDS (HIDS): A hybrid IDS is a combination of CIDS and DIDS. The IDS is placed on both centralized servers and sensing devices in the IoT environment[3].

## 4.3. IDSs focusing on attack types

IDSs developed by focusing on attack types is classified further into IDS for detecting denial of service attacks, reply attacks, Sybil attacks, wormhole attacks, false data injection attacks, and jamming attacks[3].

## 5. Machine Learning and Deep Learning for IDSs

ML, and particularly its subfield, DL, has made remarkable progress. These two fields' techniques can now analyze and learn from massive amounts of real-world data in a variety of formats[15]. Moreover, these methods have been used to solve complex problems in a variety of fields, including the security research domain[16]. Furthermore, they have been widely adopted by researchers as a solution for securing the IoT environment and showing their superiority in dealing with intrusion detection attacks[17]. In general, ML is split into three subdomains: supervised, unsupervised, and reinforcement learning.

Supervised learning necessitates labeled data for training. It determines the link between the data and its class, while unsupervised learning is used when labeled data is unavailable. Reinforcement learning is a feedback-based technique. Several machine learning methods have been proposed for accurate intrusion detection. Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Logistic Regression (LR), k-Nearest Neighbour (kNN), Random Forest (RF), and Artificial Neural Networks (ANN) are the most commonly used methods.

In 2006, Deep Learning methods appeared and have since emerged as a popular research subject. The term "deep" refers to many hidden layers in the neural network. It is an ANN subcategory with more hidden layers than traditional neural networks, which goes up to 150. DL deals with algorithms that learn from examples the same as in ML. As the size of the data increases, so does the performance of the ML and DL algorithms. DL algorithms require a large amount of data to find network patterns, whereas ML algorithms require less data[16].

DL methods are categorized into supervised learning and unsupervised learning. Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) comes under the category of supervised learning, and Auto-Encoder(AE)and Deep Belief Network (DBN) comes under the

category of unsupervised learning. Multiple DL methods for accurate intrusion detection have been proposed. The most common methods are as follows: CNN, Long short-Term Memory (LSTM), Deep Neural Network(DNN).

## 6. Evaluation metrics of IDSs

Generally, metrics such as recall, false positive, false negative, precision, f-measure, and accuracy are used to evaluate and compare the performance of developed IDS models[18].TABLE 1 summarizes the four possible outcomes of a detection.

**Table 1**  
Confusion Matrix

		Predicted	
		Normal	Attack
Actual	Normal	True Negative	False Positive
	Attack	False Negative	True Positive

- True Positive (TP) - Attack data correctly classified as an attack.
- False Positive (FP) - Normal data incorrectly classified as an attack.
- True Negative (TN) - Normal data correctly classified as normal.
- False Negative (FN) - Attack data incorrectly classified as normal.

Accuracy is the number of correct classifications out of all samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

The recall determines the number of correct classifications that are penalized by missing records.

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

The false alarm calculates the percentage of benign events that are incorrectly classified as malicious.

$$FRP = \frac{FP}{FP + TN} \quad (3)$$

The precision is calculated by dividing the number of correct classifications by the number of incorrect classifications.

$$precision = \frac{TP}{FP + TP} \quad (4)$$

The F-Measure is a derived effectiveness measurement that calculates the harmonic mean of precision and recall.

$$F - Measure = 2 * \frac{precesion * recall}{precesion + recall} \quad (5)$$

## 7. IDS Related Works

Numerous IDSs have been presented by researchers in recent years to detect potential attacks in IoT networks. One of the most important methods used in the development of IDS is artificial intelligence-based modeling. Therefore, this section analyzes some previous works in this field.

This work [18], proposes a network intrusion detection system (NIDS) by using a non-symmetric deep auto-encoder for unsupervised feature learning and the SVM classification algorithm to identify network traffic as known attacks or normal data. The authors validated the proposed NIDS's effectiveness on the KDD Cup'99 dataset, achieving high accuracy and low false alarms.

In [19], the authors used the ReliefF algorithm to select features from the Windows 10 dataset. and applied deep learning and machine learning techniques to classify the data as normal or attack data. The algorithms applied are KNN, SVM, neural networks, and LSTM, and their results were 98.93%, 98.22%, and 97.97%, respectively.

The authors in [20], presented an improved IDS using Gradient Boosting (GB) and DT through the open-source Catboost framework in the feature engineering step. The proposed model has been evaluated on the NSL-KDD, IoT-23, BoT-IoT, and Edge-IIoT datasets and obtained good scores for the performance metrics of accuracy, recall, and precision.

In [21], the authors provided a deep feature extraction (DFE) NIDS based on a CNN, with a focus on low-processing-power devices. The efficacy of the proposed model has been evaluated using three datasets: UNSW-NB15, CICIDS2017, and KDDCup99, and their results were 100%, 99.915%, 98.98%, respectively. The model was tested for both binary and multi-class classifications.

In [22], a hybrid intrusion detection model for wireless IoT networks using a CNN with a DT classifier has been presented. The DT algorithm is used as a classifier in the IoT network to classify deep features and detect attacks. The benchmark NSL-KDD dataset is used to validate the performance of the proposed intrusion detection model. This model achieved a high degree of accuracy.

In this study [23], a deep-convolutional neural network (DCNN)-based IDS for malicious activity identification in IoT networks was proposed and evaluated on the IoTID20 dataset. The performance of the proposed model was tested for binary, multi-class categories, and multi-class subcategory classifications.

In [24], the stacked autoencoder method was used in the study to reduce dimensionality, and the Gaussian Mixture Model-based Wasserstein Generative Adversarial Network (GMM-based WGAN) algorithm was used to deal with the imbalanced classes in the NSL-KDD and UNSW-NB15 datasets. The Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) module was tested on the given datasets and obtained remarkable accuracy.

In this study [25], a hybrid approach using a set of machine learning algorithms and a set of deep learning models has been proposed for the detection of DDoS attacks in IoT networks. The datasets used for the experimentation are BOT-IoT and the TONIoT network dataset. The model obtained a significant rate of accuracy.

In this study [26], a CNN-based approach for anomaly-based IDS has been proposed to improve the IoT network's performance and security. The datasets used for the experimentation were NID and BOT-IoT, which achieved 99.51% and 95.55% accuracy, respectively.

In [27], an intelligent IDS capable of detecting abnormal behavior on insecure IoT networks is developed by combining feature dimensionality reduction Principal Component Analysis (PCA)

and machine learning methods (XgBoost, Cat Boost, KNN, SVM, and Quadratic Discriminant Analysis (QDA)).The proposed model's effectiveness was validated using the UNSW-NB15 dataset. The model was 99.9% accurate.

In [28],the authors present Realguard, a DNN-based NIDS that operates directly on local gateways to accurately detect a wide range of cyber attacks in network traffic. The authors validated the effectiveness of the proposed NIDS on the CICIDS2017 dataset. The model was tested for both binary and multi-class classifications, and achieved high detection accuracy.

In [12], an ensemble-based intrusion detection model (logistic regression, NB, and DT) has been proposed for feature selection with a voting classifier, and the effectiveness of the proposed model has been evaluated using the CICIDS2017 dataset. The model was tested for both binary and multi-class classifications and achieved a significant improvement in accuracy.

This work [29], proposes a framework system to detect intrusions in the IoT environment. The authors applied three DL models to classify the intrusion: a CNN, LSTM, and a hybrid convolution neural network with the CNN-LSTM model. The IoTID20 dataset has been used for the evaluation of these DL models.The studies discussed in this section are summarized comparatively in TABLE 8.

## 8. Discussion

The development of IDS based on various ML and DL approaches has been the main focus of research studies to address security and privacy challenges in IoT networks. Researchers have developed their proposed solutions with those techniques.

From a dataset point of view, UNSW-NB15, BOT-IOT, CICIIDS2017, and NSL-KDD datasets are the most frequently used by the researchers. The proposed approaches give different performances depending on the selected datasets and the input characteristics.However, The same learning approaches and techniques do not always yield the same outcomes for a wide range of possible attack classes. For example, using the CICIIDS2017 dataset, the authors in [28] found a performance accuracy of 99.93%,while using the same dataset, the authors in [21] found a 98.98% accuracy, and both papers used DL techniques for intrusion detection.The BOT-IOT dataset achieved 100% performance accuracy in [20] and 88% accuracy in [25].Both of these papers used machine learning in their solutions.Whereas the UNSW-NB15 dataset achieved significant performance accuracy of 100%, in[21] using a deep learning technique and 99.9% performance accuracy in [27]using machine learning techniques. The NSL-KDD datasets achieved 99.81% performance accuracy in [20] using machine learning techniques and 86.59% performance accuracy in [24] using a deep learning techniques.

Binary classification is the task of classifying the elements of a set into two groups (each called a class); in the case of an IDS, these two classes are "normal" or "attack".Furthermore, multiclass classification is the problem of classifying instances into one or three or more classes. In this field (IDS), the classes represent the normal and attack categories, which vary from one dataset to another. These classes include Denial-of-Service (DoS), MIArai, and MITM ARP Spoofing,Reconnaissance Attacks.Moreover, for multiclass-subcategory classification, each category of attack cited above has various more-specific subcategories of attack methods. A DoS attack, for example, can also be a distributed DoS (DDoS) attack, a smurf attack, a TCP



SYN attack, or a DoS-Synflooding attack.

The intrusion detection process is a classification problem, so the researchers used ML and DL methods to classify intrusions from normal data. The accuracy results mentioned in the table are very acceptable, and as a result, the majority, if not all, of these ML or DL solutions produce effective results and perform satisfactorily. The TABLE 8 below was discussed in this section.

## 9. Conclusion

With the development of attacks that threaten the security of the IoT and the limitations of the IoT in terms of storage and processing, traditional intrusion detection techniques have not become effective, and the development of solutions commensurate with this situation has become inevitable, particularly new solutions enhanced by artificial intelligence, in order to be able to suppress these attacks.

The two most popular fields of artificial intelligence (AI), namely DL models and ML algorithms for binary and multiple classifications, are used in the design of a large number of IDSs.

In this article, we began by discussing the IoT concept and the challenges facing its security, as well as one of the security solutions, IDS. In addition, we conducted a comparison of ML and DL approaches for IDSs for the IoT. We first analyzed numerous articles and compared ML and DL techniques, datasets, classification granularity, and performance indicators. We extracted the pros and cons of each study. As a result, we found that CNN, SVM, LSTM, and DT are the most commonly used for attack detection..

In the future, we plan to propose a new approach to IDS for securing the IoT using ML, DL, or a hybrid of the two techniques. taking into account the actual challenges of related systems and ensuring better performance.

## References

- [1] G. D. Maayan, The iot rundown for 2020: Stats, risks, and solutions, [urlhttps://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx](https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx), 2020.
- [2] C. Benali, R. Maamri, A hybrid architecture based on blockchain to ensure security, privacy, and trust in iot, *International Journal of Organizational and Collective Intelligence (IJOI)* 12 (2022) 1–23.
- [3] S. Santhosh Kumar, M. Selvi, A. Kannan, et al., A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things, *Computational Intelligence and Neuroscience* 2023 (2023).
- [4] A. A. Anitha, L. Arockiam, A review on intrusion detection systems to secure iot networks, *International Journal of Computer Networks and Applications* 9 (2022) 38–50.
- [5] N. M. Kumar, P. K. Mallick, The internet of things: Insights into the building blocks, component interactions, and architecture layers, *Procedia computer science* 132 (2018) 109–117.

- [6] J. Pacheco, D. Ibarra, A. Vijay, S. Hariri, Iot security framework for smart water system, in: 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), IEEE, 2017, pp. 1285–1292.
- [7] B. Cherif, Z. Sahnoun, M. Ramdane, B. Nardjes, Internet of things: Security between challenges and attacks, in: Machine Learning for Networking: Second IFIP TC 6 International Conference, MLN 2019, Paris, France, December 3–5, 2019, Revised Selected Papers 2, Springer, 2020, pp. 444–460.
- [8] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, B. Stiller, Landscape of iot security, *Computer Science Review* 44 (2022) 100467.
- [9] P. Nayak, G. Swapna, Security issues in iot applications using certificateless aggregate signature schemes: An overview, *Internet of Things* (2022) 100641.
- [10] Cia triad definition. examples of confidentiality, integrity, and availability, [urlhttps://www.wallarm.com/what/cia-triad-definition](https://www.wallarm.com/what/cia-triad-definition), 2022.
- [11] A. Khraisat, A. Alazab, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, *Cybersecurity* 4 (2021) 1–27.
- [12] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, J. Ahmad, A new ensemble-based intrusion detection system for internet of things, *Arabian Journal for Science and Engineering* (2021) 1–15.
- [13] M. Ozkan-Okay, R. Samet, Ö. Aslan, D. Gupta, A comprehensive systematic literature review on intrusion detection systems, *IEEE Access* 9 (2021) 157727–157760.
- [14] C. A. de Souza, C. B. Westphall, R. B. Machado, L. Loffi, C. M. Westphall, G. A. Geronimo, Intrusion detection and prevention in fog based iot environments: A systematic literature review, *Computer Networks* (2022) 109154.
- [15] G. Nguyen, S. Dlugolinsky, M. Bobák, V. Tran, Á. López García, I. Heredia, P. Malík, L. Hluchý, Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey, *Artificial Intelligence Review* 52 (2019) 77–124.
- [16] G. Kocher, G. Kumar, Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges, *Soft Computing* 25 (2021) 9731–9763.
- [17] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, M. Nasser, Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review, *Applied sciences* 11 (2021) 8383.
- [18] M. Imran, N. Haider, M. Shoaib, I. Razzak, et al., An intelligent and efficient network intrusion detection system using deep learning, *Computers and Electrical Engineering* 99 (2022) 107764.
- [19] R. H. Mohamed, F. A. Mosa, R. A. Sadek, Efficient intrusion detection system for iot environment, *International Journal of Advanced Computer Science and Applications* 13 (2022).
- [20] M. Douiba, S. Benkirane, A. Guezzaz, M. Azrou, An improved anomaly detection model for iot security using decision tree and gradient boosting, *The Journal of Supercomputing* (2022) 1–20.
- [21] A. Basati, M. M. Faghih, Dfe: Efficient iot network intrusion detection using deep feature extraction, *Neural Computing and Applications* 34 (2022) 15175–15195.
- [22] J. Simon, N. Kapileswar, P. K. Polasi, M. A. Elaveini, Hybrid intrusion detection system for

wireless iot networks using deep learning algorithm, *Computers and Electrical Engineering* 102 (2022) 108190.

- [23] S. Ullah, J. Ahmad, M. A. Khan, E. H. Alkhamash, M. Hadjouni, Y. Y. Ghadi, F. Saeed, N. Pitropakis, A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering, *Sensors* 22 (2022) 3607.
- [24] J. Cui, L. Zong, J. Xie, M. Tang, A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data, *Applied Intelligence* (2022) 1–17.
- [25] S. A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for ddos attacks in lightweight iot networks, *Expert Systems with Applications* 215 (2023) 119330.
- [26] T. Saba, A. Rehman, T. Sadad, H. Kolivand, S. A. Bahaj, Anomaly-based intrusion detection system for iot networks through deep learning model, *Computers and Electrical Engineering* 99 (2022) 107810.
- [27] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, R. Colomo-Palacios, A machine learning-based intrusion detection for detecting internet of things network attacks, *Alexandria Engineering Journal* 61 (2022) 9395–9409.
- [28] X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh, K.-H. Le, Realguard: A lightweight network intrusion detection system for iot gateways, *Sensors* 22 (2022) 432.
- [29] H. Alkahtani, T. H. Aldhyani, Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms, *Complexity* 2021 (2021) 1–18.

**Table 2**

A comparison of existing work related to intrusion detection

Study	Year	Techniques Used	Dataset	Accuracy	Classification Granularity	Pros	Cons
[18]	2022	SAE+SVM	KDD Cup'99	99.65%	Multiclass	-High detection accuracy. -reduces computational and time costs. -low false alarm 1.92%.	-Applied only on one dataset. -There was no simulation in the study. -Performance is lower with two classes.
[19]	2022	ReliefF Medium neural network Weighted KNN Fine Gaussian SVM LSTM	ToN-IoT-Windows	98.39% 98.22% 97.97%	Binary	-High detection accuracy.	-The experimentation on one dataset. -No multiclass or multiclass-subcategory classification. -There was no simulation in the study.
[20]	2022	Gradient Boosting Decision Tree	NSL-KDD IoT-23 BoT-IoT Edge-IIoT	99.81% 99.98% 100% 100%	Binary Multiclass	-Low cost in time. -High detection accuracy. -The study is supported by simulation.	-Not applied for multiclass-subcategory.
[21]	2022	DFE based CNN	UNSW-NB15 KDD Cup99 CICIDS2017	100% 99.915% 98.98%	Binary Multiclass	-High detection accuracy. -Processing power is limited.	-Not applied for multiclass-subcategory classification. -There was no simulation in the study.
[22]	2022	CNN Decision Tree	NSL-KDD	99.49%	Multiclass	-High accuracy -The study is supported by simulation.	-Applied only on one dataset -Not applied for binary classification
[23]	2022	CNN DNN	IoTID20	99.84% 98.12%	Binary Multiclass Multiclass-subcategory	-High detection accuracy for binary and multiclass classification.	-low accuracy for multiclass subcategory classification. -There was no simulation in the study.
[24]	2022	SAE (CNN-LSTM)	NSL-KDD UNSW-NB15	86.59% 87.70%	Multiclass	-Remarkable accuracy.	-Applied just for multiclass classification. -There was no simulation in the study.
[25]	2023	Linear SVM- Naive Bayes Logistic Regression ANN LSTM	BoT-IoT TON-IoT	88-99%	Binary	-Significant detection rate for DDoS attack.	-Applied just for binary classification. -There was no simulation in the study.
[26]	2022	CNN	BoT-IoT NID	95.55% 99.51%	Multiclass	-High detection accuracy.	-Only for multiclass classification. -Few types of attacks. -There was no simulation in the study.
[27]	2022	XGBooST, CatBooST, KNN, SVM, QDA	UNSW-NB15	99.9%	Multiclass	-High detection accuracy.	-Evaluated on one dataset. -Only for multiclass classification. -There was no simulation in the study.
[28]	2022	DNN	CICIIDS2017	99.93%	Binary Multiclass	-Low resource consumption. -Detect cyber attacks in real time. -High detection accuracy. -Operates on resources-constraint gateways.	-Vulnerable to adversarial attacks. -The experimentation on one dataset.
[12]	2021	Decision Tree, Naive Bayes Logistic Rregression Voting classifier	CICIIDS2017	88.92% 88.96%	Binary Multiclass	-significant detection accuracy -low computational power, resources and low false alarm.	-Evaluated only on one dataset. -There was no simulation in the study.
[29]	2021	CNN LSTM CNN-LSTM	IoTID20	98.4%	Binary	-New real dataset generated from the IoT environment. -Detect real-world attacks.	-Only for bianry classification. -Applied on one dataset.