Internet of Things and Cyber-Physical Systems 4 (2024) 110–128

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

# Deep learning for cyber threat detection in IoT networks: A review

Alyazia Aldhaheri, Fatima Alwahedi, Mohamed Amine Ferrag *, Ammar Battah

*Technology Innovation Institute, 9639, Masdar City, Abu Dhabi, United Arab Emirates*

ARTICLE INFO

*Index Terms:*
Cyber threats
Deep learning
Intrusion detection
IoT
Machine learning

ABSTRACT

The Internet of Things (IoT) has revolutionized modern tech with interconnected smart devices. While these innovations offer unprecedented opportunities, they also introduce complex security challenges. Cybersecurity is a pivotal concern for intrusion detection systems (IDS). Deep Learning has shown promise in effectively detecting and preventing cyberattacks on IoT devices. Although IDS is vital for safeguarding sensitive information by identifying and mitigating suspicious activities, conventional IDS solutions grapple with challenges in the IoT context. This paper delves into the cutting-edge intrusion detection methods for IoT security, anchored in Deep Learning. We review recent advancements in IDS for IoT, highlighting the underlying deep learning algorithms, associated datasets, types of attacks, and evaluation metrics. Further, we discuss the challenges faced in deploying Deep Learning for IoT security and suggest potential areas for future research. This survey will guide researchers and industry experts in adopting Deep Learning techniques in IoT security and intrusion detection.

## 1. Introduction

The Internet of Things (IoT) is an emerging industry that will significantly change how we use technology and the physical environment. By 2025, it is expected that there will be 30 billion IoT-connected devices. As the number of connected devices grows, so does the risk of data breaches caused by IoT gadgets' frequently inadequate processing and storage capabilities [1,2]. Since IoT devices often have limited computational power and storage, they can be vulnerable to invaders as the IoT grows. Improvements in mobile technology have paved the way for the proliferation of the IoT, reshaping fields including healthcare, real estate, and smart cities [3]. These linked devices are smart gadgets that use network interface cards and lightweight central processing units managed by many interface services. The IoT can potentially impact our collective future as technology develops significantly. The rapid growth of the IoT has made security one of the most critical issues in a networked, interdependent system. Hackers, viruses, and other harmful software could compromise the safety and reliability of data. In addition, data insecurity has the potential to directly undermine the security of the entire IoT and usher in several perilous circumstances [4–6]. Robust IoT security solutions are, therefore, in high demand. As the number of IoT devices grows and new risks appear, it will become increasingly important to gather and analyze data to maintain the safety of these gadgets. Because of this, IoT security has emerged as a top priority. Existing security methods include, but are not limited to, systemic security architecture and cryptographic security mechanisms. Network attacks, such as a flood of requests to IoT services quickly or unauthorized access to particular services, could have severe repercussions [7,8]. Therefore, installing intrusion detection systems (IDSs) to identify malicious actors and maintain the availability and safety of IoT networks is crucial. However, complex IDSs are rarely useable due to IoT devices' limited resources and power. An intrusion detection system monitors a network's health and activity. An alert is issued to the network administrator once an intrusion is discovered [9]. When dealing with different volumes and incorrect sequences of event streams, conventional IDSs' architecture, built essentially to handle the Internet's priority management characteristics, falls short [10].

The IoT has profoundly impacted our daily lives by connecting billions of devices and producing massive amounts of data. However, this rapid growth of IoT networks has prompted new security concerns due to the inherent vulnerabilities of IoT devices [11]. To detect and block malicious activity, an IDS is crucial for protecting IoT networks. Rule-based IDS methods have traditionally been used, but the complexity and diversity of IoT networks have rendered them inefficient. Deep learning is one approach that could be used to improve the efficiency and precision of IDS for IoT devices. To maximize the use of IDSs in the IoT using deep learning and further identify the flaws and strengths of these systems, it is essential to evaluate the available literature and

* Corresponding author.
*E-mail addresses:* alyazia.aldhaheri@tii.ae (A. Aldhaheri), fatima-alwahedi@hotmail.com (F. Alwahedi), mohamed.ferrag@tii.ae (M.A. Ferrag), ammar.battah@tii.ae (A. Battah).

https://doi.org/10.1016/j.iotcps.2023.09.003
Received 5 September 2023; Received in revised form 23 September 2023; Accepted 30 September 2023
Available online 10 October 2023

publications extensively. Despite the importance of intrusion detection systems (IDSs) in IoT, they have not yet been the subject of systematic, in-depth study [8]. Therefore, this essay critically examines everything published in 2019–2023. In this study, we classify existing IDSs in the IoT, assess several intrusion detection methods, and summarize our findings. Moreover, many researchers struggle to locate comprehensive and trustworthy datasets to test and evaluate their proposed approaches, which is a significant problem in and of itself. To test the efficacy of such methods, we need publicly available datasets that include both benign and numerous attacks, meet real-world requirements, and are reliable [12].

The present study investigates existing and prospective strategies for protecting IoT systems from extensive attacks. To achieve this objective, it is imperative to comprehend IoT systems comprehensively, examine past instances of extensive attacks that have disrupted IoT systems, and evaluate the diverse approaches researchers have suggested or executed to protect them.

The purposes of this paper are as follows.

- Surveying state-of-the-art work and relevant topics in the field comprehensively.
- Examination of recent surveys tackling methods for detecting cyber threats and put into comparison.
- Investigating and comparing works based on DL approaches for threat detection and recent ML approaches.
- Evaluating the available IoT datasets, giving a detailed analysis of each with their issues and advantages.
- Exploring the different attacks and threats on IoT devices.
- Discussing the current unresolved issues and challenges in this field.

The rest of the paper is organized as follows: Section II provides an overview of related survey papers focusing on Intrusion Detection Systems (IDSs). Section III contains an overview of related Deep Learning Approaches for Intelligence Detection utilized throughout the article. Section IV displays the available datasets for IoT. Section V discusses the attacks and threats on IoT. Lastly, in section VI the conclusion is presented.

### 1.1. Search strategy

Conducting a comprehensive research review necessitates diligently searching for the most pertinent studies about the chosen research topic. To identify pertinent scholarly research about our subject matter, we used the research tools available through Google Scholar. Google Scholar is a frequently utilized tool for extensively exploring scholarly literature. A rigorous selection process was implemented to ensure the rigor of this research review, wherein only publications published in journals with readily accessible full text were included. Google Scholar is a comprehensive platform encompassing various academic publications and sources, such as IEEE, Springer, Science Direct, SCOPUS, and Wiley. Table 1 displays the search queries employed in retrieving articles from Google Scholar about the application of deep learning techniques in the field of cyber security, specifically in the context of intrusion detection for IoT security.

### 1.2. Method of selection

We have evaluated those papers based on the following criteria.

**Table 1**
Search criteria.

| Key | Input |
|---|---|
| Search string | (IoT OR “internet of things”) AND Security AND (“Deep Learning for Security”) |
| Year Range | Article date between 2019 and 2023 |

- The initial and crucial step is selecting papers related to the topic.
- It is recommended to assess the h-index of a paper, as it measures both its productivity and impact in the field. Additionally, it is essential to check whether the paper has been published in respected journals. This will help to ensure that the research being reviewed is of high quality and credibility.
- It is advisable to focus on those published between 2019 and 2023, as this will help identify the most recent research on the subject. This ensures that the information being reviewed is up-to-date and relevant to current trends and developments in the field.
- It is important to consider the originality of the papers being reviewed. Look for papers introducing new ideas or methods to address a specific problem. Such papers may have received awards or recognition for their contributions to the field. By focusing on original research, you can better understand the latest developments and innovations in the subject area.
- When conducting research, it is advisable to search for papers cited the most by other researchers, as this indicates their significance and impact in the field. Such papers are considered the most influential works in their respective areas of study. The higher the overall score assigned to a source, the higher it was ranked on the list, indicating its relative importance and relevance to the research topic. This approach helped to streamline the review process and ensure that the most valuable and informative sources were given the most attention.

### 1.3. Quality assessment questionnaire

When selecting papers, it is important to consider whether they are relevant to the topic at hand. Additionally, to help assess the quality of the papers, certain questions can be asked.

- Are the research topic and proposed solution relevant to our research
- Does the paper clearly explain the data collection process?
- Does the paper state its objective?
- Does the research compare different learning methods?

## 2. Related surveys

IDS has emerged as a viable approach to safeguarding networks and information systems in cybersecurity. Researchers have been concentrating on developing innovative and efficient intrusion detection systems for IoT. Recently, several investigations have investigated the utility of DL-based and ML-based IDS for enhancing IoT security. This section presents related surveys and provides comparisons as shown in Table 2.

The survey utilized a comparison analysis, and an overview of deep learning algorithms for cyber security intrusion detection is presented by Ferrag et al. [13] review IDSs based on deep learning techniques. They analyzed seven deep learning models: recurrent neural networks, convolutional neural networks, deep belief networks, limited Boltzmann machines, and deep autoencoders. They investigated the performance of two real-world traffic datasets in binary and multiclass classification categories, specifically the CSE–CIC–IDS2018 and the Bot-IoT datasets.

To ensure the security of computer networks, Da Costa et al. [14] focuses on current, rigorous, state-of-the-art machine learning techniques used in IoT and intrusion detection. With a focus on the IoTs and machine learning, the study intends to conduct a thorough and contemporary analysis of pertinent works that deal with various intelligent approaches and their applicable intrusion detection structures in computer networks. Over 95 papers on the topic were reviewed, covering various topics relating to security challenges in IoT systems. In this study, the scientific and industrial communities’ key concerns and efforts have concentrated on creating optimum security protocols that provide enough protection while consuming minimal energy. Several clever strategies are also presented in the paper and applied to the context of computer network security, including intrusion detection.

The IoT NIDS deployed by machine learning is the objective of

**Table 2**
Comparison of related surveys.

| Year | Authors | Focused security domain | DL/ML methods | Evolution performance | Attacks on IoT | Description of IoT Dataset | Considered Timeline |
|---|---|---|---|---|---|---|---|
| 2019 | *Ferrag* et al. | Cyber security IDs | DL and ML | ✓ | X | ✓ | (2015–2019) |
| 2019 | *Da Costa* et al. | IDs and NIDs | ML | ✓ | X | X | (2013–2018) |
| 2019 | *Chaabouni* et al. | NIDs | ML | ✓ | ✓ | ✓ | (1999–2018) |
| 2019 | *Hajiheidari* et al. | IDs | DL and ML | ✓ | ✓ | ✓ | (2009–2019) |
| 2020 | *Asharf* et al. | IDs and NIDs | DL and ML | ✓ | ✓ | ✓ | (2011–2019) |
| 2020 | *Ahmad* et al. | NIDs | DL and ML | ✓ | X | ✓ | (2017–2020) |
| 2021 | *A. Khraisat and A. Alazab* | IDs | DL and ML | ✓ | ✓ | ✓ | (2009–2019) |
| 2022 | *Tsimenidis* et al. | IDs | DL | ✓ | X | ✓ | (2016–2020) |
| 2022 | *Jayalaxmi* et al. | IDs and IPs | DL and ML | ✓ | X | X | (2013–2021) |
| 2023 | *This survey* | IDs | DL | ✓ | ✓ | ✓ | (2019–2023) |

Chaabouni et al. [15]'s survey since learning algorithms have demonstrated significant success in security and privacy. In contrast to other leading surveys focusing on traditional systems, the survey offers a thorough analysis of NIDSs using various learning techniques for the Internet of Things. IoT dangers and detection methods have been categorized compared to conventional protection mechanisms. Then, an exhaustive evaluation of NIDS implementation tools is presented, beginning with freely available network datasets, open-source network traffic monitoring tools, and open-source NIDS. Academics and businesses can leverage these resources to create and evaluate advanced NIDS solutions.

In the context of IoT ecosystems, Hajiheidari et al. [16] have suggested a thorough review of IDSs. Similarly, they have evaluated several highly developed intrusion detection in the IoT and clarified and analyzed unresolved concerns through an in-depth examination of over 40 important research among the fundamental 324 publications. Based on the available literature, the articles were divided into three categories—centralized, distributed, and hybrid—and four basic categories: signature-based IDS, specification-based IDS, anomaly-based IDS, and hybrid IDS. Moreover, nine forms of assaults (DoS/DDoS, Sybil, selective forwarding, black hole, sinkhole, jamming, replay, fake data, wormhole) and two areas of evaluation (theoretical, simulation) are considered. Additionally, it discussed the benefits and drawbacks of many IDSs. To create IDSs that are more effective in the future, the problems with existing methodologies are addressed.

A review of IDS for IoT networks and systems that employ ML and DL-based intrusion detection approaches was provided by Asharf et al. [17] Discussed the IoT architecture, protocols, IoT system vulnerabilities, and IoT protocol-level attacks. Moreover, various research studies published in the literature proposed IDS methodologies for IoT or attack detection techniques for IoT that could be included in an IDS, focusing on different ML and DL techniques made available for IoT IDS and their use by researchers.

Ahmad et al. [18] offer new researchers a comprehensive understanding of the current knowledge, recent trends, and progress in network intrusion detection mechanisms that employ ML and DL methods, achieved through an extensive review. The process of choosing pertinent articles in the domain of AI-based NIDS is carried out systematically. Their study encompasses assessing a concise data set, performance evaluations of models, and the prevailing trends in IDS. The article identifies the research gaps regarding enhancing model performance for infrequent attacks in real-world scenarios and simplifying security. It underscores future research challenges dating a NIDS framework that employs simpler deep learning algorithms yet retains effective intrusion detection capabilities. The goal is to develop a lean and efficient deep learning-based NIDS for identifying network intruders, drawing on the insights garnered from this study.

Ansam Khraisat and Ammar Alazab [19]. provided a comprehensive article that offers an in-depth evaluation of the state-of-the-art IoT IDS and a summary of the techniques, deployment tactics, validation procedures, and datasets widely employed to develop IDS. In addition, they analyzed how current IoT IDS identifies invasive attacks and safeguards IoT connections. The study also categorizes IoT threats to enhance IoT security and underscores future research challenges needed to counter these risks. A special IoT IDS taxonomy clarifies IoT IDS methods, their advantages and drawbacks, IoT attacks that use IoT communication networks, and matching improved IDS and detection capabilities to identify IoT assaults.

Tsimenidis et al. [20] presented a survey containing the models for IoT intrusion detection that were provided with the specific tasks they were used for and the results they produced. Also, it was discussed why deep learning is a better approach for IDSs than shallow machine learning models and the difficulties this new paradigm confronts. Despite the advantages of deep learning compared to other approaches for IoT intrusion detection, there is significant potential for further research. Developing distributed deep-learning-based IDS systems could address the requirements of large-scale, distributed, and self-organizing IoT networks. Additionally, creating more computationally efficient models would better support resource-constrained devices.

Jayalaxmi et al. [21] conduct research on risk factor analysis utilizing a mapping approach and offer a hybrid framework concept for an effective security model for intrusion detection (ID) and prevention. Moreover, it has examined the value of various Artificial Intelligence (AI)-based strategies, tools, and procedures for IoT detection and prevention systems. For intrusion detection and prevention systems, it focused more explicitly on Machine Learning (ML) and DL approaches. It provided a comparative study on viability, compatibility, difficulties, and real-time concerns. This survey assists both businesses and academics in analyzing the problems and concerns with the current security models and developing new directions for security framework innovations using effective ML or DL techniques.

## 3. Approaches for cyber threat Intelligence Detection

Many papers published in IoT are not assessed in the reviewed literature. Thus, it is essential to note that the current study stands out from previously published articles due to its rigorous selection process, analysis of diverse and credible databases, and the sheer number of articles reviewed.

IDS is a potential cyber security protection strategy for networks and information systems. Academic research has been focused on creating novel, effective, and efficient intrusion detection systems for IoT. Several studies have explored using DL-based IDS for IoT security in recent years. This section analyzes prior studies utilizing novel and traditional deep learning techniques for securing IoT environments. Fig. 1 provides an overview of the discussed approaches proposed by recent works. Table 3-C summarizes the various methods employed, their performance, and the datasets used in these studies.

### 3.1. Deep Learning Approaches

Recent works are increasingly employing deep learning models and

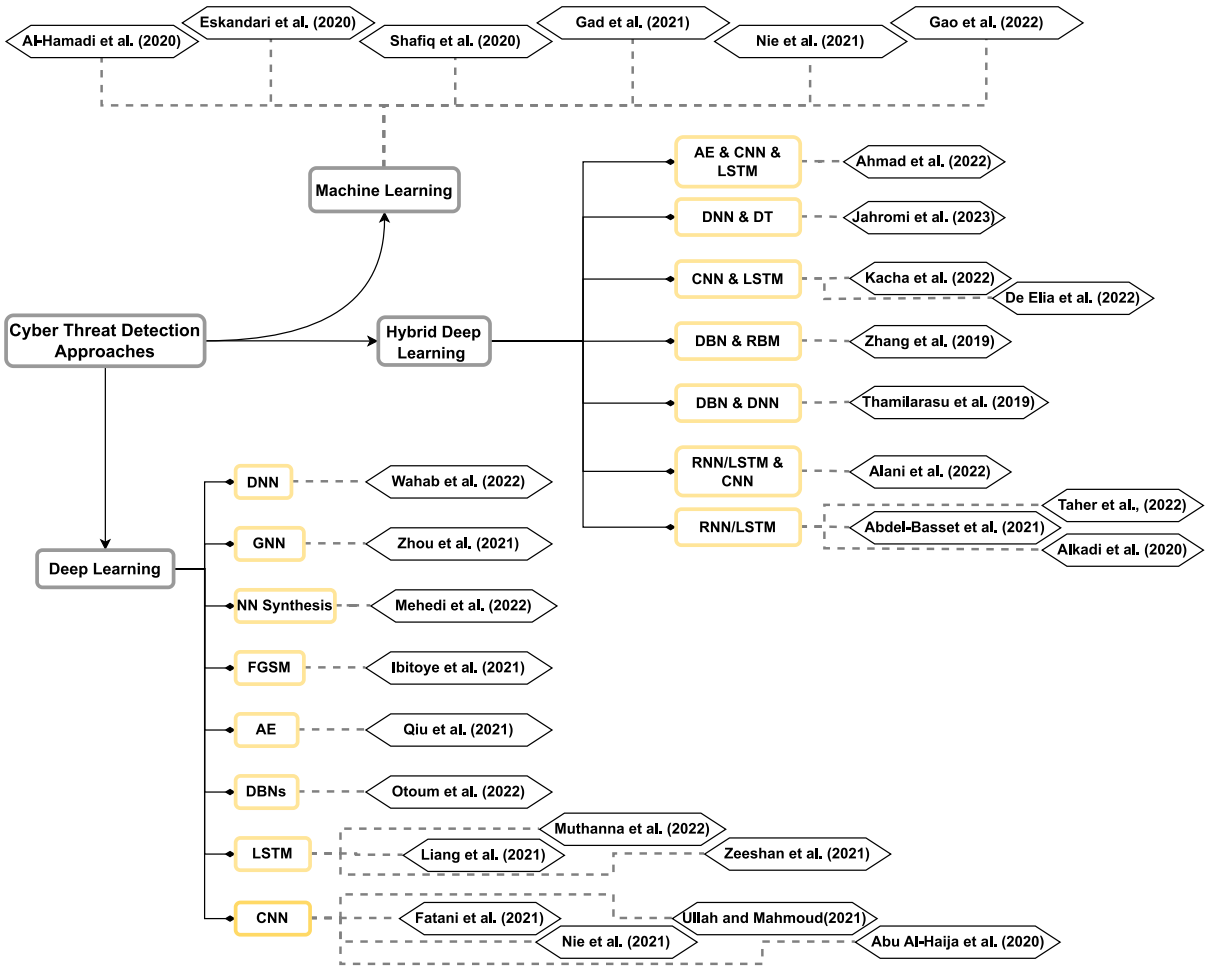


**Fig. 1.** Cyber threat detection approaches proposed by recent works based on category and technique.

methods for threat detection. We delve into the recent works in this field based on the model and approach utilized.

A novel feature selection method was developed based on the TSODE algorithm, which is an enhanced version of the transient search optimization (TSO) algorithm introduced by Fatani et al. [22]. The efficacy of the devised method was tested using four public datasets: KDDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017. These datasets were used for multi-classification and binary classification scenarios, encompassing a variety of attack types including Web-based, interaction, heart-bleed, brute-force, DoS, and DDoS attacks. The multi-classification results demonstrated accuracies of 92.06 % for KDDCup-99, 75.75 % for NSL-KDD, 99.04 % for BoT-IoT, and 99.93 % for CICIDS-2017. For binary classification, the accuracies were 99.99 % for BoT-IoT, 92.45 % for KDDCup-99, 77.38 % for NSL-KDD, and 99.99 % for CICIDS-2017.

Nie et al. [23] proposed a data-driven Intrusion Detection System (IDS) to analyze the link load patterns of the Road Side Unit (RSU) in the Internet of Vehicles (IoV) during different attacks causing significant traffic flow variations. For capturing the link load characteristics and detecting intrusions aimed at RSUs, a deep learning architecture rooted in convolutional neural networks (CNN) was implemented. This design merges a conventional CNN with a basic error term, thus enhancing the convergence of the training algorithm. A testbed emulating an IoV environment was constructed, featuring 30 OBUs and a single RSU. The paper's assessments, under various conditions, revealed that the accuracy of the CNN in a setting with 12 OBUs reached 97.60 %.

Ullah and Mahmoud [24] introduced a novel anomaly-based intrusion detection model tailored for IoT networks. This multiclass classification system model harnesses convolutional neural networks (CNNs) capabilities in 1D, 2D, and 3D architectures for classification tasks. The efficacy of this CNN model was validated using several datasets: BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23. When juxtaposed with extant deep learning models, the proposed binary and multiclass classifications displayed superior accuracy, notably benefitting from transfer learning.

A breakdown of accuracies for multiclass classification on different datasets is as follows.

- BoT-IoT: CNN1D - 99.97 %, CNN2D - 99.95 %, CNN3D - 99.94 %.
- IoT Network Intrusion: CNN1D - 97.76 %, CNN2D - 97.55 %, CNN3D - 97.08 %.
- MQTT-IoT-IDS2020: CNN1D - 99.93 %, CNN2D - 99.93 %, CNN3D - 99.92 %.
- IoT-23: CNN1D - 99.96 %, CNN2D - 99.90 %, CNN3D - 99.84 %.

Moreover, the IoT-DS-2 dataset was chosen for pre-training, encompassing both typical network traffic and all attacks from the other datasets. The achieved accuracy for binary classification using IoT-DS-2 was CNN1D - 99.96 %, CNN2D - 99.98 %, and CNN3D - 99.98 %.

Ullah and Mahmoud [24] introduced a novel anomaly-based intrusion detection model tailored for IoT networks. This model is a multiclass classification system that employs the convolutional neural network (CNN) architectures in 1D, 2D, and 3D for its classification tasks. The model's effectiveness was tested on several datasets: BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23. When juxtaposed with extant deep learning models, both the proposed binary and multiclass classifications exhibited remarkable accuracy, notably benefitting

**Table 3**
Deep learning approaches for cyber threat intelligence detection.

| Authors | Ref. | Year | Method | Dataset | Performance | Open Issues |
|---|---|---|---|---|---|---|
| Fatani et al. | [22] | 2021 | TSODE | KDDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017 | Multi-classification: BoT-IoT = 99.04 %, KDDCup-99 = 92.06 %, NSL-KDD = 75.75 % and CICIDS-2017 = 99.93% | An open issue for the transient search optimization-based system for secure IoT is the scalability of the system |
| Nie et al. | [23] | 2020 | CNN | Created testbed | Acc = 97.60 %. | Trained exclusively for RSUs, not tested on published data and is limited to Binary classification |
| Ullah and Mahmoud | [24] | 2021 | CNN1D, CNN2D, and CNN3D models | BoT-IoT, IoT, Network Intrusion, MQTT-IoT-IDS2020 and IoT-23 | Multiclass classification: CNN1D = 99.97 %, CNN2D = 99.95 %, CNN3D = 99.94 % | Lack of detailed performance analysis in terms of prediction and training time |
| Abu Al-Haija et al. | [46] | 2020 | IoT-IDCS-CNN | NSL-KDD | Acc = 98.2–99.3 % (98.75 % average) | Lack of testing in an applicable real-world application with a real-time environment |
| Liang et al. | [25] | 2021 | OICS-VFSL | NSL-KDD and CIC-IDS 2017 | NSL-KDD = 91 %. | Ensuring low latency and high throughput for data transmission |
| Muthanna et al. | [26] | 2022 | Cu-LSTM-GRU | CICIDS2017 | Cu-LSTM-GRU = 99.23 % | Tested only on a partial dataset (CICIDS2017) with five classes, lack of experimentation for a network-based IDS |
| Zeeshan et al. | [27] | 2021 | PB-DID | UNSW-NB15 and Bot-IoT | Acc = 96.3 % | Lack of attack variety (DoS/DDoS considered only) |
| Otoum et al. | [28] | 2022 | DL-IDS | NSL-KDD | Acc = 99.02 % | Developing a communication protocol that can support end-to-end encryption, mutual authentication, and authorization |
| Qiu et al. | [29] | 2020 | ID-Based NIDS | Mirai | Acc = 94.31 % | Need for further experimentation and analysis by attacking different NIDS |
| Ibitoye et al. | [30] | 2019 | FNN IDS and SNN IDS | BoT-IoT | FNN ≈ 51 % and SNN ≈ 51 % | Further investigation on different models and attacks, and providing insights on how to improve them |
| Mehedi et al. | [31] | 2022 | P-ResNet | Own dataset (by capturing network traffic) | Acc = 87 % | Lacks description about the size of the dataset |
| Zhou et al. | [32] | 2021 | HAA | UNSW-SOSR2019 | Precision ≈ 30 % | Specific study for GNN models for hierarchal IoT network, needs to be expanded upon |
| Abdel Wahab et al. | [33] | 2022 | Principal component analysis (PCA) | DS2OS | Acc ≈ 99.23 % | Solution needs to be tested in a dynamic environment to realistically capture the desired results rather than using a static dataset. Only local information considered |
| Alkadi et al. | [34] | 2020 | Deep blockchain framework (DBF) | UNSW-NB15, BoT-IoT | UNSW-NB15 = 97.26 %, BoT-IoT = 96.71 % | BiLSTM-based systems are typically computationally expensive due to their recurrent nature and the need to process sequential data |
| Taher et al. | [35] | 2022 | TSA-LSTMRNN | KDD Cup99 | Acc = 92.67 % | Precision for U2R is extremely low (41.63 %). Can only be utilized by non-uniform distribution of class labels. |
| Abdel-Basset et al. | [36] | 2021 | SS-Deep-ID | CIC-IDS2017 and CIC-IDS2018 | Binary classification: CIC-IDS2017 = 99.6 % and CIC-IDS2018 = 99.33 % | Needs real-world applicable experimentation for online deployment in a dynamic environment rather than a static dataset |
| Alani et al. | [37] | 2022 | Two-layer IoT IDS | IoT network intrusion dataset | Acc = 99.15 % | The two classifiers were tested and evaluated separately but is crucial to test the complete system when deployed "Online" and gauge its performance |
| Thamilarasu et al. | [38] | 2019 | IIDS | Own dataset (by capturing network traffic) | Precision rate = 95 % | Complex setup and high computational cost, handles binary classification(each attack tested separately) |
| Zhang et al. | [39] | 2019 | GA-DBN | NSL-KDD dataset | Acc ≈ 98.82 % | No IoT traffic was used, focusing on four general attacks. Lack of temporal performance experimentation and analysis |
| Elias et al. | [40] | 2022 | Improved hybrid CNN-LSTM | Edge-IIoTset dataset | Binary classification = 97.85% Multiclass classification = 97.14 % | Lack of temporal performance analysis and experimentation, as well as real-world application experimentation |
| Khacha et al. | [41] | 2022 | Hybrid CNN-LSTM | Edge-IIoTset dataset | Binary classification = 100% Multiclass classification = 98.69 % | No deep insight into training time and the overhead due to integration of two models, cost analysis requires further expansion |
| Jahromi et al. | [42] | 2023 | Cyber-threat hunting | Secure Water Treatment (SWaT) and Gas pipeline dataset | Secure Water Treatment (SWaT): Centralized = 95.15 % and Federated = 95.12 % Gas pipeline dataset: Centralized = 99.64 % and Federated = 99.66 % | Need for security analysis as federated learning introduces new security risks. Thorough experimentation of the complexity and cost of deployment is required |
| Ahmad et al. | [43] | 2022 | Ensemble (no name) | CICIDS2017, BoT_IoT, N_BaIoT, NSL-KDD | CICIDS2017 = 76.18 %, BoT_IoT = 75.10 %, N_BaIoT = 99.97 %, NSL-KDD = 27.96 % | Performs poorly on several classes, requires further improvement to deal with unique unknown attacks |
| Al-Hamadi et al. | [44] | 2020 | ADIoTS | IoT network intrusion dataset (The 128-sensor carrying mobile IoT devices) | N/A | Complex model for nodes and need for further empirical results |
| Eskandari et al. | [45] | 2020 | Passban | Own dataset (by capturing network traffic) | iForest = 96.6 % and LOF = 88.25 %. | Security concern due to system reliance on fog/edge nodes. Empirical data of real-world application needed to validate approach |

(*continued on next page*)

**Table 3** (*continued*)

| Authors | Ref. | Year | Method | Dataset | Performance | Open Issues |
|---|---|---|---|---|---|---|
| Gad et al. | [47] | 2021 | VANETs | ToN-IoT dataset | Binary classification = 98.2 %<br>Multi-classification = 97.9 % | General dataset used for specific application, lack of temporal and spatial performance analysis in a critical application |
| Shafiq et al. | [48] | 2020 | CorrAUC | BoT-IoT | Acc = 99.99% | Need for experimentation of approach with deep learning techniques |
| Gao et al. | [49] | 2022 | BSBC-RF | SCADA Network dataset (Industrial traffic) | Acc = 99.96 % | Only applicable for binary classification, and applied for ML algorithms only (rather than DL) |
| Nie et al. | [50] | 2021 | DDPG | CICDDoS2019 | Precision rate = 99.14 % | Binary classification of DDoS attacks exclusively |

from transfer learning. For the BoT-IoT dataset, the accuracies in multi-class classification were 99.97 % for CNN1D, 99.95 % for CNN2D, and 99.94 % for CNN3D. For the IoT Network Intrusion dataset, the respective accuracies were 97.76 %, 97.55 %, and 97.08 %. In the MQTT-IoT-IDS2020 dataset, the figures stood at 99.93 % for both CNN1D and CNN2D, and 99.92 % for CNN3D. In the IoT-23 intrusion detection dataset, CNN1D achieved 99.96 %, CNN2D 99.90 %, and CNN3D 99.84 % in multiclass classification. Furthermore, the IoT-DS-2 dataset, which encompasses both standard network traffic and all attacks from the other datasets, was selected for pre-training. Here, the binary classification accuracy was 99.96 % for CNN1D, 99.98 % for CNN2D, and 99.98 % for CNN3D.

#### 3.1.1. Long short-term memory (LSTM)

Liang et al. [25] enhanced the microservice-oriented intrusion detection in distributed IoT systems. They employed the Optimized Intra/Inter-Class-Structure-Based Variational Few-Shot Learning (OICS-VFSL) models to address a particular out-of-distribution challenge in unbalanced learning scenarios. To evaluate the efficacy of their proposed approach, experiments were conducted on two public datasets: NSL-KDD and CIC-IDS 2017. The NSL-KDD dataset comprises four attack classes, namely: U2R, R2L, Probe, and DoS. In contrast, the CIC-IDS 2017 dataset encompasses eleven distinct attacks: HeartBleed, DoS, DDoS, XSS, SQL Injection, Brute Force, Botnet, Infiltration, FTP-Patator, PortScan, and SSH-Patator. Results from the study indicated that the OICS-VFSL model achieved an accuracy of approximately 91 % for adversarial samples.

To address the challenges of threat identification in IoT environments, Muthanna et al. [26] introduced an intelligent SDN-enabled hybrid architecture leveraging the Cuda Long Short-Term Memory Gated Recurrent Unit (cuLSTMGRU). For comparative evaluation, the performance of the proposed model was juxtaposed with cuBLSTM and cuGRUDNN on the same IoT-centric dataset. State-of-the-art IoT datasets along with established assessment metrics were utilized. Additionally, they incorporated two hybrid classifiers to juxtapose their results with the cuLSTMGRU for a more comprehensive evaluation. The efficacy of the constructed model was assessed against a diverse set of DOS attacks, encompassing SYN, UDP Flood, UDP Scan, and Ping Flood, using a distributed performance matrix. The CICIDS2017 dataset was employed for accuracy assessment. The proposed cuLSTMGRU approach yielded an accuracy of 99.23 %, outperforming the cuBLSTM and cuGRUDNN which achieved 97.31 % and 96.97 % accuracy rates, respectively.

Zeeshan et al. [27] proposed Protocol Deep Intrusion Detection (PB-DID) architecture. Feature clusters in both data sets were constructed based on flow and domain. Notably, the predominant features fall into the flow and TCP clusters. The methodology encompasses feature selection, data pre-processing, and data selection from the UNSW-NB15 and Bot-IoT datasets. Additionally, an unsupervised LSTM deep learning model is utilized for training. The architecture identifies four types of attacks, with the bulk of the dataset primarily consisting of DoS and DDoS packets. PB-DID employs two distinct output layers: one for binary classification and another for multi-class classification. In terms of performance, PB-DID achieves an accuracy of 99.4 % for binary classification and 96 % for multi-class classification.

#### 3.1.2. Deep belief networks (DBNs)

Otoum et al. [28] introduced a cutting-edge Deep Learning-based Intrusion Detection System (DL-IDS) that integrates the Spider Monkey Optimization (SMO) algorithm with the Stacked-Deep Polynomial Network (SDPN). The system achieves a notable enhancement in detection accuracy by selecting optimal dataset features using SMO and subsequently employing SDPN for data classification. The DL-IDS effectively identifies anomalies, including Denial of Service (DoS), User to Root (U2R), probing, and Remote-to-Local (R2L) attacks. Upon evaluation using the NSL-KDD dataset, the system exhibited an impressive accuracy of 99.02 %.

### 3. Autoencoders (AE)

Qiu et al. [29] introduced a novel adversarial technique targeting DL-based network intrusion detection systems (NIDSs) within the IoTs environment. Their approach exploits only black-box access to the DL models within such NIDSs. The strategy comprises two main steps: 1) leveraging model extraction to replicate the black-box model with minimal training data, and 2) employing a saliency map to illustrate the influence of individual packet attributes on detection outcomes and highlight key features. The system's efficacy was tested on the Mirai dataset, revealing that adversaries could achieve a success rate surpassing 95 %.

#### 3.1.4. Generative adversarial networks (FGSM)

Ibitoye et al. [30] compares the performance of the FNN with the Self-normalizing Neural Network (SNN) for categorizing intrusion attacks in an IoT network, the SNN is a variation of the FNN. This study aims to determine how a deep learning-based IDS for IoT may enhance performance accuracy in the context of adversarial samples. The BoT-IoT dataset from the UNSW Canberra Cyber Center is used for the study. According to the evaluation, the SNN IDS is more resistant to adversarial attacks than the FNN IDS. In contrast to SNN, which had an accuracy of around 32 %, FNN had an accuracy of around 23 %. The SNN IDS performed 9 % more accurately than the FNN IDS on average when faced with adversarial data.

#### 3.1.5. Neural network synthesis (NNs)

Mehedi et al. [31] introduced dependable DTL-based residual neural network (P-ResNet) IDS. This system can efficiently train even with a limited set of target domain data and operates with minimal computational overhead. Furthermore, the P-ResNet model demonstrates enhanced performance as the network depth increases. The dataset comprises data from seven distinct IoTs sensors, including the GPS tracker, motion light sensor, garage door sensor, Modbus sensor, thermostat sensor, weather sensor, and fridge sensor. The proposed P-ResNet detection model boasts an impressive accuracy rate of 87 %, signifying reliability and computational efficiency.

#### 3.1.6. Graph neural networks (GNN)

Zhou et al. [32] introduced the Hierarchical Adversarial Attack (HAA) generation technique to facilitate a level-aware black-box adversarial attack strategy. This method targets GNN-based intrusion detection in IoT systems, even under budgetary constraints. The efficacy of the HAA generation method is evaluated using the UNSW-SOSR2019

open-source dataset and benchmarked against three conventional techniques. The results underscore the potency of the proposed method: it can notably diminish the classification accuracy of two state-of-the-art GNN models, namely GCN and JK-Net, by over 30 %, when juxtaposed with the three benchmark methods.

#### 3.1.7. Deep neural network (DNN)

Wahab et al. [33] introduced a drift detection technique leveraging the PCA methodology to study the variance shifts in features across intrusion detection data streams. The work elaborates on an online DNN that dynamically adjusts its hidden layer sizes based on the Hedge weighting algorithm. This adaptation empowers the model to continuously learn and adapt to new intrusion data. The performance of this approach was benchmarked against a conventional DNN using the Distributed Smart Space Orchestration System (DS2OS) traffic traces dataset. The proposed model showcased an average accuracy of 99.23 %, surpassing the standard DNN.

### 3.2. Hybrid approaches

#### 3.2.1. Recurrent neural network (RNN) based on LSTM

Alkadi et al. [34] introduced a deep blockchain framework (DBF) tailored for enhancing security in IoT networks. This framework integrates a security-centric distributed intrusion detection system with a privacy-oriented blockchain that incorporates intelligent contracts. They employed a bidirectional long short-term memory (BiLSTM) deep learning approach to process sequential network data. The experiments were conducted on the UNSW-NB15 and BoT-IoT datasets, encompassing a range of attacks, including DoS TCP, DoS UDP, DoS HTTP, DDoS TCP, DDoS UDP, and DDoS HTTP. The findings indicate an optimal hidden node size of 10, yielding an accuracy of 97.26 % for the UNSW-NB15 dataset and 96.71 % for the BoT-IoT dataset.

Taher et al. [35] proposed the Tunicate Swarm Algorithm (TSA-LSTMRNN) model to detect attacks in IoT settings. They fine-tuned hyper-parameters using TSA, enhancing the detection efficacy of the long-short-term memory-recurrent neural network (LSTMRNN) model. The model's performance was benchmarked using the KDD Cup99 Dataset, which includes data segmented into five categories: DoS, R2L, normal, U2R, and Probe. Comparative evaluations revealed that the TSA-LSTMRNN model outperformed prior models, achieving an accuracy rate of 92.67 %.

Abdel-Basset et al. [36] introduced a semi-supervised deep learning strategy for intrusion detection, termed *SS-Deep-ID*, which incorporates a multiscale residual temporal convolutional (MS-Res) module. During its training phase, *SS-Deep-ID* exploits the features from labeled and unlabeled traffic sequences to detect intrusions or cyberattacks within traffic data generated by IoT networks. The classification is performed in both binary and multiclass settings. To evaluate the efficacy of their approach, the researchers employed two contemporary datasets: CIC-IDS2017 and CIC-IDS2018. For binary classification, *SS-Deep-ID* achieved an accuracy of 99.6 % on the CIC-IDS2017 dataset and 99.33 % on the CIC-IDS2018 dataset. In the multiclass setting, the respective accuracies were 99.69 % and 98.71 %.

#### 3.2.2. RNN with CNN and LSTM

Alani et al. [37] explored the domain of IoT security and presented an innovative two-layer intrusion detection approach for IoT. This architecture synergistically leverages both flow-based and packet-based features, with machine learning algorithms bolstering its intelligence. The essence of the introduced system is its ability to meld flow-based and packet-based characteristics, aiming for elevated detection precision. The IoT network intrusion dataset was opted for, primarily because the system mandates both packet and flow data. This dataset encompasses raw network packets sourced from actual IoT devices and incorporates attack-induced traffic. The authors formulated a pipeline containing five distinct classifiers, each tailored for the dataset and trained on its respective training subset. The classifiers employed were xGradient Boost (XGB), Random Forest (RF), Decision Tree (DT), Gaussian Naive Bayes (GNB), and Logistic Regression (LR). Upon evaluation, the proposed methodology manifested an impressive accuracy rate of 99.15 %.

#### 3. Deep belief networks (DBN) and DNN

Thamilarasu et al. [38] introduced an intelligent intrusion-detection system (IIDS) tailored for the IoT environment. This IDS is designed to detect network activity anomalies and segment the traffic into distinct sessions. The IIDS interfaces with routers and other IoT devices through network virtualization, promiscuously monitoring and analyzing network traffic continuously. For the anomaly detection process (ADP), the authors developed a unique dataset derived from meticulous data collection and preprocessing. When tested against five specific attack scenarios—sinkhole, wormhole, DDoS, opportunistic service attack, and blackhole-the system exhibited an average precision of 95 % and a recall of 97 %, as evidenced by the precision-recall curves.

#### 3.2.4. DBN and restricted Boltzmann machine (RBM)

Zhang et al. [39] integrated the Deep Belief Network (DBN) with an enhanced genetic algorithm (GA). The refined GA, employing multiple iterations, constructs an optimal network structure. The DBN then employs this structure as an intrusion detection model for classifying attacks. The methodology was validated using simulations on the NSL-KDD dataset, and the proposed GA-DBN approach yielded an average detection rate accuracy of 98 % for four distinct types of attacks.

#### 3.2.5. Hybrid convolutional neural networks (CNN) and LSTM

Elias et al. [40] introduced a neural network model incorporating a hybrid CNN-LSTM architecture to detect diverse network attacks at the edge of the Industrial Internet of Things (IIoT). Notably, the detection is based solely on features derived from the transport and network layers, bypassing the application layer information. Modifications to the original architecture include adding two dense layers and a flattening layer positioned before the final dense layer, enhancing the model's performance. The Edge-IIoTset dataset, highlighting features from the TCP, ICMP, UDP, and ARP protocols (instead of HTTP, MQTT, DNS, and ModBus protocols), was used for evaluation. The model achieved superior performance with an average binary classification accuracy of 97.85 % and a multiclass classification accuracy of 97.14 % compared to other models.

In the work of Khacha et al. [41], a system harnessing both CNN and LSTM was proposed. These techniques are particularly potent for intrusion detection and classification due to their aptitude for feature classification and swift computation. The latest dataset, Edge-IIoTset, which contains authentic traffic data from various IoT devices, was employed to evaluate the model's efficacy. Their CNN-LSTM model demonstrated superiority over solely LSTM-based and traditional machine learning models, especially in cybersecurity intrusion detection for IIoT applications. The CNN-LSTM model achieved an average accuracy of 100 % in binary classification and 98.69 % in multiclass classification.

#### 3.2.6. DNN and DT

Jahromi et al. [42] introduced an ensemble-driven deep federated learning approach for cyber threat hunting. This model aims to inspect attack samples without the necessity of data sharing. The hunting model consists of two concurrent federated components: the first evaluates the IIoT status based on the network's regular condition. In contrast, the second scrutinizes it in light of potential threat scenarios. The generalizability of the proposed model is tested using two distinct scenarios. For the initial test, the model leverages the secure water treatment (SWaT) dataset from real-world water purification processes. The model's efficacy is gauged in the subsequent test using four distinct gas pipeline datasets. Remarkably, the proposed model surpassed competing models in both centralized and federated settings. It achieved an accuracy of 95.15 % in a centralized configuration and 95.12 % in a federated one.

#### 3.2.7. AE with CNN and LSTM

Ahmad et al. [43] introduced an innovative IDS technique rooted in the ensemble of deep learning classifiers. This method was trained on four benchmark IDS datasets to identify unfamiliar attack scenarios. Their proposition hinges on the idea that a holistic intrusion detection system cannot be achieved merely through an optimal single or hybrid classifier. Instead, they amalgamated three classifiers—LSTM, CNN, and autoencoder—each distinguished for managing sequential data. Performance assessment was conducted using four benchmark IDS datasets, comprising two IoT-specific and two non-IoT-specific datasets. The model's accuracy surpassed its predecessors, registering 76.18 % on the CICIDS2017 dataset, 75.10 % on the BoT IoT dataset, 99.97 % on the N BaIoT dataset, and 27.96 % on the NSL-KDD dataset.

### 3.3. Machine learning approaches

Al-Hamadi et al. [44] utilized Stochastic Petri Net (SPN) modeling methods to develop an analytical model for assessing the interactions between intrusion detection attack-defense mechanisms within an autonomous distributed Internet of Things system (ADIoTS). In the ADIoTS, every node is mandated to perform its assigned tasks and uphold Intrusion Detection System (IDS) responsibilities to ensure system security. The research leverages an experimental dataset from a reference autonomous distributed IoT system comprising 128 mobile nodes embedded with sensors.

On the other hand, Eskandari et al. [45] introduced Passban, a smart IDS designed to protect IoT devices directly connected to it. It learns from the inherent characteristics of typical IoT traffic. Passban is a platform-independent, anomaly-based IDS that operates directly on edge devices. In its development, the researchers incorporated the isolation forest (iForest) — an algorithm premised on isolation, and the local outlier factor (LOF) — a profiling-based method. This research generated its own dataset by capturing network traffic from a home-based testbed. The study involved executing four different attack types against the AGILE gateway: port scanning, SYN flood, SSH brute force, and HTTP brute force, recording both inbound and outbound raw traffic. Employing the F1 measure, both LOF and iForest accurately identified the aforementioned attacks. The iForest method achieved an average accuracy of 96.6 %, whereas LOF registered an accuracy of 88.25 %.

Gad et al.[47] introduced an Intrusion Detection System (IDS) for VANETs, underpinned by several data preparation and preprocessing methodologies. The research relied on the ToN-IoT network records for both training and testing. Its key features distinguish this model and integrate Chi2 and SMOTE as preprocessing techniques, notably enhancing the results. The ToB-IoT dataset encompasses a variety of attack vectors such as ransomware, DoS, password attacks, DDoS, scanning, XSS, data injection, backdoor, and MITM. Using XGBoost, impressive results were achieved in binary and multi-class classification tasks. Specifically, the binary classification accuracy reached 98.2 %, while multi-classification stood at 97.9 %.

In their work, Shafiq et al. [48] introduced CorrAUC, a novel feature selection algorithm. Inspired by the wrapper technique, this algorithm adeptly filters and selects features vital for the designated machine learning (ML) model. The Area Under the Curve (AUC) metric directs the selection process, ensuring the optimal choice of features. A combination of TOPSIS and Shannon's entropy, rooted in the bijective soft-set approach, was employed to validate the features intended for malicious traffic detection in the IoT network. The research leveraged the Bot-IoT dataset and assessed four distinct ML algorithms to scrutinize the proposed method's efficacy in detecting cyberattacks within IoT networks. Remarkably, the C4.5 ML algorithm, when applied to the chosen feature set, showcased an astounding accuracy of 99.9 % in detecting Bot-IoT attacks, indicating superior performance.

Gao et al. [49] proposed an intrusion detection methodology for industrial CPSs, dubbed the border-line SMOTE and EBC learning rooted in Random Forest (BSBC-RF). BSBC-RF was benchmarked against eight state-of-the-art intrusion detection algorithms using the SCADA Network dataset to validate its efficacy. The empirical results revealed that the BSBC-RF outperforms its counterparts on most evaluation metrics, registering an impressive accuracy rate of 99.96 %.

Nie et al. [50] put forth a DDPG-based intrusion detection mechanism tailored to bolster the security landscape of green IoT. The anomaly-based intrusion detection system zeroes in on DDoS attacks by harnessing traffic flow attributes intrinsic to a green IoT environment. The evaluation framework for this method incorporated the CICDDoS2019 dataset, segmented into two sub-datasets, shedding light on novel DDoS attack vectors targeting TCP/UDP-based application layers like portmap, NetBIOS, and LDAP. Preliminary evaluations corroborate the system's prowess, evidencing a precision rate of 99.14 % in predicting network traffic patterns and pinpointing intrusions.

## 4. Available datasets

In recent years, the field of IoT security has seen the emergence of numerous datasets, each with its own set of advantages and disadvantages. As the pool of undetected vulnerabilities and threats continues to expand, there is a growing emphasis by researchers on datasets related to IoT. IoT devices' performance, security, and relevance, whether under typical or anomalous conditions, are assessed through data collection in either simulated or genuine environments. Consequently, the dataset's quality is pivotal in creating a robust model for real-world intrusion detection. While many studies predominantly use datasets like the KDD Cup 1999, NSL-KDD, and UNSW-NB15, other datasets can also serve the purpose of cyber security intrusion detection. This section delves into publicly available datasets recommended for intrusion detection systems (IDS) within IoT scenarios. Table 4 presents various datasets, highlighting their technical specifications, the layers in which they are organized, and attributes that provide comprehensive information about them.

### 4.1. KDDCUP99

The KDDCup99 dataset, used in the Third International Knowledge Discovery and Data Mining Tools Competition [51], is designed to differentiate between ”malicious” and ”benign” network connections for the development of a robust NIDS. Derived from the DARPA dataset, KDDCup99 comprises approximately 4.9 million connection records, each represented by 41 features. Each connection is categorized as either an attack or normal. The dataset encompasses various security attacks, including DoS, U2R, R2L, and Probing Attacks.

### 4.2. NSL-KDD

Introduced by Tavallaee et al. [51], the NSL-KDD dataset is a refined version of the KDDCup99 dataset. Retaining the same features as KDDCup99, NSL-KDD was curated by removing redundant and repetitive records and optimizing the dataset size. This dataset features 41 attributes along with a class label. The class label is segmented into 21 categories, further grouped into four primary attack types: probe, U2R, R2L, and DoS.

### 4.3. UNSW-NB15

Developed by the Australian Centre for Cyber Security in their Cyber–Range Lab using the IXIA PerfectStorm tool, the UNSW-NB15 dataset [52] aims to capture a blend of genuine normative behaviors with synthetically generated contemporary cyber attacks. The dataset comprises 2,540,044 records, of which 2,218,761 are benign, and 321, 283 are malicious. The dataset encompasses nine distinct attack types: backdoors, fuzzers, analysis, shellcode, DoS, exploits, reconnaissance, worms, and generic.

**Table 4**
Summary of the Reviewed Datasets'. T = Total Number of records, N = Normal number of records and M = Malicious number of records.

| Year | Dataset | Testbed type | Tools used for collection | Layers | Attacks | Features | # of records | Advantage | Open issues |
|---|---|---|---|---|---|---|---|---|---|
| 1999 | KDDCUP99 | MIT Lincolin Labs | N/A | N/A | Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L). | 41 features related to: Time, connection, content, host-based | T = 4,900,000 N = 1,033,372 M = 4,176,086 | Adopted for traditional network | Old dataset, pattern redundancy, non-stationarity between training and test datasets, highly skewed targets, and irrelevant features Multiple missing records No cloud computing service |
| 2009 | NSL-KDD | MIT Lincolin Labs | N/A | N/A | DoS, Probe, U2R, and R2L | 41 features related to: Time, connection, content, host-based | T = 1,074,992 N = 812,814 M = 262,178 | No duplicate records in the proposed test sets No redundant records in the train set compared to KDD99 | It does not represent the modern low footprint attack scenarios, lacks in modern large-scale attacks No cloud computing service Lack of public data sets for network-based IDS |
| 2015 | UNSW-nb15 | The Cyber Range Lab of UNSW Canberra | IXIA PerfectStorm tool | Client layer, Network layer, Server layer | Reconnaissance, Shellcode, Exploit, Fuzzers, Worm, DoS, Analysis and Generic | 49 features related to: Flow, content, time, basic, additional generated | T = 2,540,044 N = 2,218,761 M = 321,283 | It provides hybrid real modern normal activities and synthetics contemporary attack behaviors | No ransomware attacks |
| 2017 | CICIDS2017 | Canadian Institute for Cybersecurity (CIC) | CICFlowMeter tool | Network layer, Device layer (firewall), server layer, application layer | Normal, Botnet ARES, Brute Force, Infiltration, Port Scan, Web Attack | 80 features related to: Time stamp, source and destination IPs, source and destination ports, protocols and attack) | T = 2,830,743 N = 2,273,097 M = 557,646 | Used for traditional data | Class Imbalance Improvement of the label assignment process not public |
| 2018 | Bot-IoT | Cyber Range Lab of the center of UNSW Canberra Cyber. | VM | VM | Probing/normal attacks, Denial of Service, Information theft, Reconnaissance attack (information gathering) | 45 features related to: Frame, ARP, IP, TCP, UDP | T = 73,370,443 N = 9543 M = 73,360,900 | More sophisticated as it covers IoT devices | Imbalanced nature of data Does not contain IoT telemetry data |
| 2018 | DS2OS | Virtual IoT environment | Distributed smart space orchestration system (DS2OS) | Application layer, client layer | Denial Of Service, Malicious Operation, Malicious Control, Wrong Setup, Spying, Scan, and Data Type Probing Attacks | 13 features related to: Timestamp, value, accessed node address, accessed node type, operation, destination location, destination service type, destination service | T = 357,952 N = 347,935 M = 10,017 | Is designed to address model drifts in IoT-based intrusion detection systems | Not representative of network traffic behavior |

(*continued on next page*)

**Table 4** (*continued*)

| Year | Dataset | Testbed type | Tools used for collection | Layers | Attacks | Features | # of records | Advantage | Open issues |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | address, source location, source type, source address, normal | | | |
| 2018 | CSE–CIC–IDS2018 | Communications Security Establishment (CSE) the Canadian Institute for Cybersecurity (CIC) | CICFlowMeter-V3 | Network layer, Device layer(firewall), cloud layer | Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration | 80 features related to: time stamp, source, and destination IPs, source and destination ports, protocols and attack | T = 16,233,002 N = 14,980,167 M = 1,252,835 Without redundancy: T = 15,450,706 N = 12,697,719 M = 2,752,987 | It is modifiable, extensible, and reproducible | Limited to DDoS attacks only |
| 2019 | CICDDoS2019 | UNSW Canberra Cyber | CICFlowMeter | Application layer, network layer, server layer | 12 DDoS attacks includes NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN and TFTP | 80 features related to: source IP, source Port, destination IP, destination port, protocol, and time stamp | T = 50,063,112 N = 56,863 M = 50,006,249 | Captured modern reflective DDoS attacks such as NTP, NetBIOS, SSDP, UDP-Lag, and TFTP | Heavily focused on DoS attacks |
| 2019 | UNSW-SOSR2019 | The security laboratory at the University of New South Wales | tcpdump too | Cloud layer, Network layer, Computing Layer | ARP spoofing, TCP SYN flooding, Fraggle (UDP flooding), and Ping of Death. Reflective attacks include SNMP, SSDP, TCP SYN, and Smurf | 49 features related to: packet header, flow-based, and content-based | T = 2,541,698 N = 1,361,423 M = 1,180,275 | Diversity of attack scenarios | Limited temporal scope |
| 2020 | TON-IoT | Cyber Range and IoT Labs at UNSW Canberra Cyber | VM | Edge layer, fog layer, cloud layer | Ransomware, password attack, scanning, DoS, DDoS, data injection, backdoor, Cross-site Scripting (XSS), and man-in-the-middle (MITM). | 44 features related to: connection, statistics, user attributes, and violation attributes | T = 22,339,021 N = 796,380 M = 21,542,641 | New data-driven IIoT-based More suitable for applying DTL models | Does not include IIoT traffic and intrusion assessment for various machine learning approaches Authentication and disconnection phase not found |
| 2020 | IoT-23 | Stratosphere Laboratory of the CTU | Zeek | Network layer, application layer, cloud layer | DDoS, HeartBeat, Mirai, Okiru, Torii, CC, PartOfAHorizontal, PortScan, FileDownload | 23 features related to: packet length, time between packets, packet stream, mean, variance, and skewness of packet lengths and inter-arrival times, port numbers, response codes, device type, manufacturer, and operating system | T = 325,307,990 N = 30,858,735 M = 294,449,255 | Accurately mimics a recent trend in IoT network traffic | Focused on DNS traffic for IoT context |
| 2020 | MQTT-IOT-IDS2020 | N/A | Nmap, VLC, MQTT-PWN | | Aggressive scan (Scan A), User Datagram Protocol (UDP) scan | 44 features related to: addresses and ports, | T = 3,654,006 | Recent trend in IoT network traffic | Lacks IIoT traffic |

(*continued on next page*)

**Table 4** (*continued*)

| Year | Dataset | Testbed type | Tools used for collection | Layers | Attacks | Features | # of records | Advantage | Open issues |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Network layer, cloud layer, server layer | (Scan sU), Sparta SSH brute-force (Sparta), and MQTT brute-force attack (MQTT BF) | protocol, packet length statics and flags | N = 334,318<br>M = 3,319,688 | | |
| 2022 | Edge-IIoTset | Guelma University | Node Red, Modbus of Node Red, Argus tool | Cloud Computing Layer, Network Functions Virtualization Layer, Blockchain Network Layer, Fog Computing Layer, Software-Defined Networking Layer, Edge Computing Layer, and IoT and IIoT Perception Layer | TCP SYN Flood DDoS attack, UDP flood DDoS attack, HTTP flood DDoS attack, ICMP flood, Port Scanning, OS fingerprinting, Vulnerability scanning attack, ARP Spoofing attack and DNS Spoofing attack, Cross-site Scripting attack (XSS), SQL Injection, Uploading attack Backdoor attack, Password cracking attack, and Ransomware attack | 61 features related to: IP addresses, ports, timestamp, and payload information | T = 20,780,120<br>N = 9,729,709<br>M = 11,050,411 | New data-driven IIoT-based | No spyware attack |

### 4.4. CICIDS2017

The CICIDS2017 dataset, curated by the same institution as Sharafaldin et al. [53], is a contemporary collection of various attack scenarios. The dataset was created with genuine user-generated background traffic from the B-Profile system. It captures diverse types of attacks such as DDoS, DoS, Heartbleed, Web Attack, Infiltration, Botnet, Brute Force SSH, and Brute Force FTP. The dataset employs the CICFlowMeter tool to extract eighty distinct network flow characteristics from the captured traffic.

### 4.5. BoT-IoT

The BoT-IoT dataset, crafted by Koroniotis et al. [54] at UNSW Canberra Cyber Range Lab, encompasses legitimate and malicious traffic data from simulated IoT devices. This testbed includes network devices, notably the pfSense firewall, attack and target virtual machines (VMs), and simulated IoT devices operating within VMs connected to the AWS IoT hub. With 73,370,443 network traffic records, the dataset portrays a smart house environment containing a weather station, smart fridge, smart thermostat, remotely operated garage door, and smart lights. This dataset catalogs various attacks, including keylogging, data exfiltration, OS and service scans, and DoS and DDoS attacks.

### 4.6. DS2SoS

Introduced by Pahl et al. [55], DS2SoS is a next-generation, open-source IIoT security dataset tailored for research. It aids in evaluating the efficacy of ML/DL-driven cybersecurity algorithms, especially in smart factory and city contexts. The dataset holds 357,952 samples, split into 10,017 anomalies and 347,935 regular data points. It features 13 distinct attributes and seven categories of attacks, including denial of service, malicious operation, incorrect setup, espionage, scans, and data-type probing incursions.

### 4.7. CSE–CIC–IDS2018

The CSE–CIC–IDS2018 dataset [56] was devised as a superior replacement for existing datasets limiting IDS/NIDS experimental evaluations. This dataset highlights seven diverse attack scenarios: brute force, heartbleed, botnets, DDoS web assaults, and local network infiltrations. The hypothetical target organization consists of 5 departments, 30 servers, and 420 hosts, summing up to 50 nodes in its attack blueprint. The authors extracted 80 distinctive features from computer logs and network traffic using CICFlowMeter-V3.

### 4.8. CICDDoS2019

Sharafaldin et al. [57] curated the CICDDoS2019 dataset, focusing on DDoS attacks and leveraging the publicly accessible CICFlowMeter tool from the Canadian Institute for Cybersecurity derived 80 network traffic attributes for all benign and malicious flows. This research delves into contemporary attacks executed via TCP/UDP application-layer protocols and introduces two novel attack categories: reflection-based DDoS and exploitation-based. In both, attackers exploit legitimate third-party components to obfuscate their identity. The dataset simulates user behaviors for 25 individuals across protocols like SSH, HTTP, HTTPS, FTP, and email.

### 4.9. UNSW-SOSR2019

The UNSW-SOSR2019 dataset, sourced by the University of New South Wales security lab using the tcpdump tool [58], archives traffic from 10 distinct IoT devices. This dataset chronicles benign and malicious traffic, detailing attacks such as ARP spoofing, Fraggle (UDP flooding), TCP SYN flooding, and Ping of Death. Reflective attack types,

including SNMP, TCP SYN, SSDP, and Smurf, are also cataloged.

### 4.10. ToN-IoT

Developed jointly by the Cyber Range and UNSW Canberra IoT Labs [59], the ToN-IoT dataset amalgamates data from diverse sources within a comprehensive IIoT system. This includes network traffic, Linux and Windows OS logs, and telemetry from connected gadgets. The dataset identifies many attacks: ransomware, password attacks, scans, DoS, DDoS, XSS, data injection, backdoors, and MITM attacks, to name a few. Boasting 22,339,021 records, the dataset features 44 attributes grouped into four service-profile-based categories detailing connection, user activities (e.g., DNS, HTTP, SSL), statistics, and breach characteristics.

### 4.11. IoT-23 dataset

The IoT-23 dataset, curated by the Stratosphere Laboratory of the Czech Technical University (CTU) [60], provides researchers with a comprehensive collection of genuine IoT data, including benign and malicious activities. It encompasses three benign and 20 malicious actions and 20 network operation models that mimic IoT device scenarios. The dataset comprises 325,307,990 records distributed across nine attack categories: DDoS, HeartBeat, Mirai, Okiru, Torii, C&C, PartOfAHorizontal, PortScan, and FileDownload [24].

### 4.12. MQTT-IoT-IDS2020

Hindy et al. developed the MQTT-IoT-IDS2020 dataset, which focuses on conventional and brute-force attacks targeting the MQTT networking framework [61]. This dataset captures several prevalent MQTT attack instances alongside test cases involving real devices. The network structure includes 12 MQTT sensors, an MQTT broker, a camera feed replication mechanism, and an intrusion detection system. The four primary attack types presented are Sparta SSH brute-force, User Datagram Protocol (UDP) scan, Aggressive scan (Scan A), and MQTT brute-force (MQTT BF).

### 4.13. Edge-IIoT

The Edge-IIoT dataset, introduced by the authors in Ref. [62], is designed to facilitate intrusion detection research. It enables the evaluation of federated deep learning and centralized intrusion detection systems using universally accepted metrics. The dataset describes 14 attacks associated with IoT and IIoT protocols, further classified into five threat categories: information gathering, DoS and DDoS attacks, injection attacks, malware-based attacks, and man-in-the-middle attacks. It encompasses 1176 features, with 61 of them being highly correlated. The dataset documents 20,780,120 attack-related records, of which 11,050, 411 are benign, and 9,729,709 are malicious. Traffic predictability and detection efficacy were assessed across cyber-threats using binary, 6-category, and 15-category classifications. The evaluation employed classifiers like RF, SVM, kNN, and DNN.

## 5. Evaluation metrics

Deep learning offers a myriad of metrics to evaluate the performance of classifiers. Choosing an appropriate performance metric is crucial and is predominantly governed by the practical requirements of the specific application. One primary goal in evaluating deep learning models is to enhance these performance metrics. For the scope of this discussion, we focus solely on the performance metrics sourced from the research papers we reviewed amidst the plethora of available metrics in deep learning. This section elucidates the evaluation metrics commonly adopted to assess the efficacy of intrusion detection systems that leverage deep learning techniques. The foundation for these metrics is the *Confusion Matrix*, a matrix that contrasts the actual versus the predicted class labels of the inputs. The key evaluation metrics are enumerated as follows.

- **True Positive (TP):** Instances correctly identified as attacks by the classifier.
- **False Negative (FN):** Attack instances incorrectly classified as normal by the classifier.
- **False Positive (FP):** Normal instances incorrectly classified as attacks by the classifier.
- **True Negative (TN):** Instances correctly identified as normal by the classifier.

Table 5 illustrates the relationships between the above-described elements of the confusion matrix. Furthermore, several evaluation metrics can be derived from these elements.

### 5.1. Accuracy (ACC)

Accuracy is a widely utilized metric to gauge the efficacy of classifiers, particularly in the domain of Intrusion Detection Systems (IDS). It quantifies the classifier's capability to identify intrusions or attacks correctly. Mathematically, accuracy represents the fraction of intrusion attempts correctly classified out of the total input samples.

$$ACC = \frac{TP_{\text{Attack}} + TN_{\text{Normal}}}{TP_{\text{Attack}} + TN_{\text{Normal}} + FP_{\text{Normal}} + FN_{\text{Attack}}} \tag{1}$$

### 5.2. Precision (PR)

Though accuracy provides a holistic view of a model's performance, relying on it solely can be misleading in certain scenarios. Supplementary metrics like precision (PR) are essential when accuracy is not the sole criterion for decision-making. Precision denotes the fraction of positively predicted instances that are genuinely positive. Specifically, it encapsulates the rate of correctly identified malicious packets.

$$PR = \frac{TP_{\text{Attack}}}{TP_{\text{Attack}} + FP_{\text{Normal}}} \tag{2}$$

### 5.3. Recall (R)

Recall, or sensitivity, assesses the model's ability to identify all positive instances confidently. It represents the proportion of actual malicious packets that the model correctly identifies. Ensuring a high recall is paramount as overlooking extensive attacks could result in undetected malicious traffic.

$$R = \frac{TP_{\text{Attack}}}{TP_{\text{Attack}} + FN_{\text{Attack}}} \tag{3}$$

### 5.4. F-measure (F1)

The F-measure, often denoted as $F1$ score, harmoniously combines precision and recall. It furnishes an overarching assessment of the model's performance, particularly its proficiency in pinpointing attack traffic while reducing false positives and negatives. A superior $F1$ score is indicative of enhanced model performance.

$$F1 = 2 \cdot \frac{PR \cdot R}{PR + R} \tag{4}$$

**Table 5**
Confusion matrix.

| Predicted class | | | |
|---|---|---|---|
| *Actual Class* | | **Attack** | **Normal** |
| | **Attack** | True Positive | False Negative |
| | **Normal** | False Positive | True Negative |

## 6. Threats and attacks

Over the past decade, IoT devices have faced numerous attacks, leading to heightened user apprehension regarding their usage. These malicious activities targeting IoT devices and networks are termed as IoT-based threats and attacks. The primary objectives of attackers encompass information collection, data theft, and denial of service to authentic users. With the anticipated rise of IoT-connected devices into billions by 2020, there is also an expected increase in potential vulnerabilities. The lack of standardization in IoT technologies can amplify these vulnerabilities, resulting in security breaches in IoT systems [63]. Subsequent sections delve into prevalent security challenges in IoT. This segment collates details about predominant threats and attacks within the IoT sphere. Over recent years, multiple attacks have targeted IoT devices, prompting users to exercise added caution. Attackers commonly seek information, purloin data, or inhibit services intended for genuine users. This segment elucidates specific attacks and their objectives, categorizing them into active and passive types. A broad overview of these attacks is depicted in Fig. 2. Additionally, we have compiled a table categorizing the attacks, defining them, and listing tools for their execution in Table 6.

### 6.1. Denial of service and distributed denial of service

#### 6.1.1. Denial of service

A DoS attack comprises attacks that render a service or network inaccessible to its intended audience. These attacks primarily aim to disrupt services for all users by targeting individual users or devices or by overloading network resources [64].

#### 6.1.2. Distributed denial of service

DDoS represents a multifaceted Denial of Service attack executed via compromised nodes from diverse locations. Common techniques employed by attackers include TCP SYN Flood, UDP flood, HTTP flood, and ICMP flood.

- **TCP SYN Flood:** Attackers leverage the TCP connection sequence to incapacitate a victim's network. By swiftly dispatching TCP connection requests, they intend to inundate the target system, leading to a network overload [65].
- **UDP Flood:** By deluging a target with UDP packets, it prompts the host to check for an application, causing inaccessibility repeatedly. The flood of User Datagram Protocol (UDP) packets hampers the system's capacity to process them, making it unavailable to genuine users.

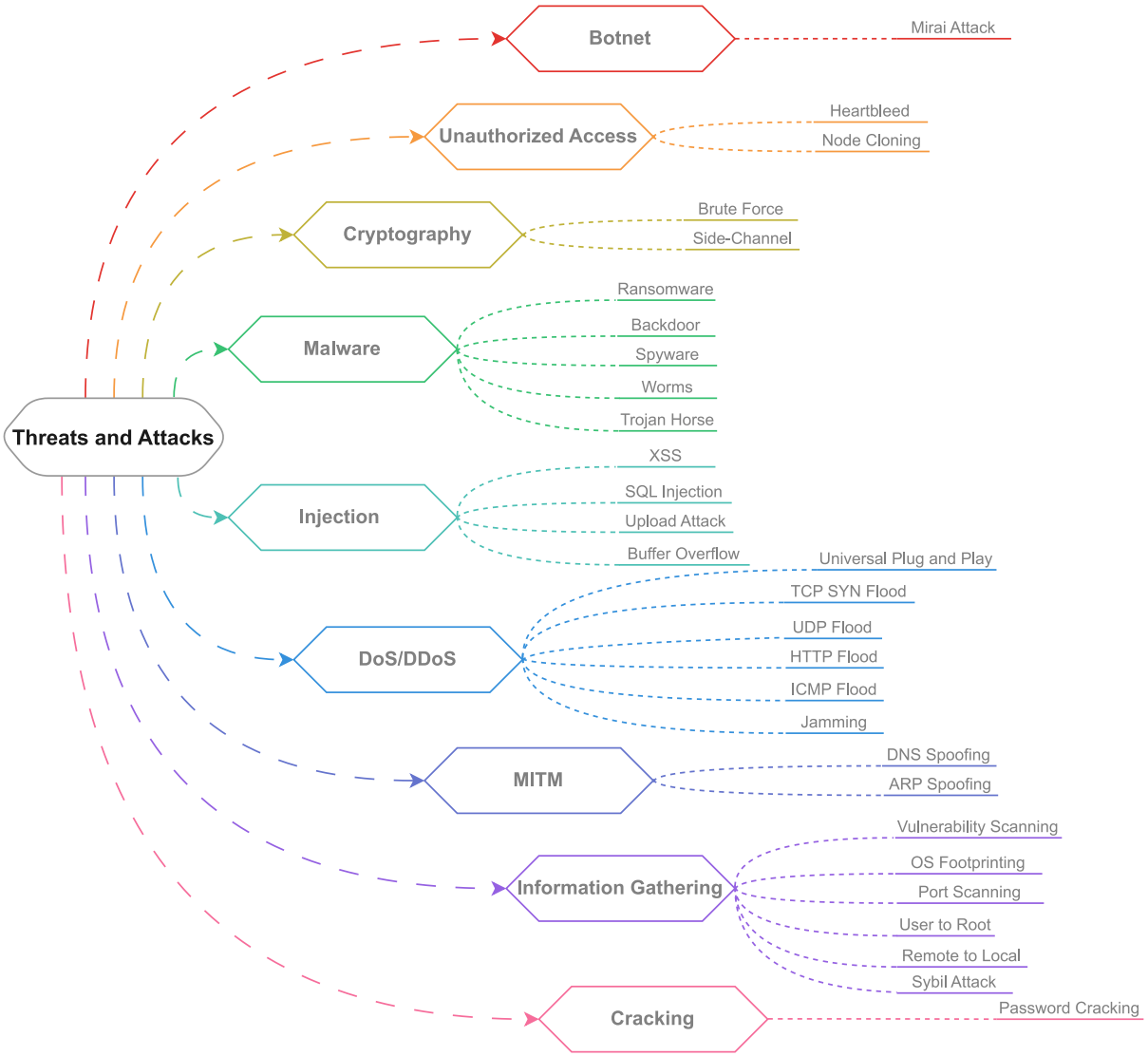


**Fig. 2.** Different categories of threats and attacks to which IoT devices are susceptible.

**Table 6**
Threats and attacks.

| Category of Attacks | Type of Attacks | Definition | Tools (most prevalent) |
|---|---|---|---|
| Denial-of-Service (DoS)/ Distributed Denial-of-Service (DDoS) | TCP SYN flood | Overwhelming its ability to handle legitimate requests, making it unavailable. | Hping3, LOIC, Slowloris |
| | UDP flood | Overwhelming IoT device process and response abilities. | hping3, LOIC, UDP Unicorn, UFONet, XOIC |
| | HTTP flood | Overburden IoT device with a large volume of HTTP requests. | LOIC, Slowhttptest, HULK, Slowloris |
| | ICMP flood | Continuous packets of ICMP Echo Request or ping packets to disturb a network's service. | hping3, LOIC, Ping To Death, Scapy |
| | Jamming | Floods noise or radio frequency interference to jam the wireless communication channel between the devices. | HackRF one, Aircrack-ng, RTL-SDR, USRP |
| | Universal Plug and Play (UPnP) | Conduct different attacks on networked devices using vulnerabilities that are in IoT devices. | UPnProxy, masscan, hping3, scapy, nmap |
| Information gathering | Vulnerability scanning | Identifying vulnerabilities or weaknesses in a IoT system. | Intruder, Detectify, Acunetix, Qualys Guard, OpenVAS |
| | OS Fingerprinting | Identifying the OS running on a target system by analyzing network traffic or other information. | PRADS, PacketFence, Nmap, XProbe2 |
| | Port scanning | Scan for ports to determine which are accessible, closed, or have a security procedure. | Nmap, NetCat, SolarWinds. ManageEngine, OpUtils |
| | User to Root(U2R) | An intruder attempts to obtain network resources as a regular user. (Unauthorized access to local superuser (root) privileges) | Attack Channels: Buffer_overflow, perl, rootkit |
| | Remote to Local (R2L) | Exploit vulnerabilities or weaknesses in remote access protocols/services to gain unauthorized access to a local system. (Unauthorized access from a remote machine) | Attack Channels: ftp_write, warezclient, phf, password_guessing, Imap, worm |
| | Sybil attack | An attacker generates many false identities in order to undermine the security or control of a network or system. | NetCat, SolarWinds, ManageEngine |
| Man-In-The-Middle attacks | DNS Spoofing | Manipulates DNS by redirect users to malicious sites or intercept their communications. | Ettercap, Dnsspoof, Arpspoof |
| | ARP Spoofing | Enables attackers to monitor network device data. | NextGenSpoofer |
| Injection attacks | Cross-site Scripting (XSS) | Injects malicious scripts into a web page to steal sensitive data or credentials. | XSStrike, XSS Hunter, XSSER. Acunetix, DalFox |
| | SQL Injection | Injecting harmful SQL commands into an app's input fields to manipulate or extract data from its database. | SQL Map. Leviathan, SQLNinja, JSQL Injector, NoSQLMap |
| | Uploading attack | Uploads malicious code on a web site to obtain illegal access or damage. | SQLNinja, JSQL Injector, NoSQLMap |
| | Buffer overflow | Data overwrites adjacent memory locations, corrupting data values. | Any programming language that can be injected on the target |
| Malware attacks | Ransomware | Takes hostage files or IoT devices by blocking access to IoT device or data. | OpenSSL, Netcraft, PCHels, WannaCry, Angler Exploit Kit, ransomware worm) |
| | Backdoor | Install a gateway to gain access to susceptible IoT network devices. | Metasploit, Netcat, Empire, Aircrack |
| | Spyware | Installs program without consent to monitor and gather information. | SpyEye, Blackshades, FlexiSPY, NetWire |
| | Worms | Replicates itself on IoT system, spreading to other systems and causing damage by (Delete data/Steal data/take control) | CodeRed, Mydoom, WannaCry, Sasser Worm, Stuxnet |
| | Trojan horses | Acts like legitimate software and performs (export files, modify data, delete files or altering the contents) | Zeus, Remote Access Trojan (RAT), Back Orifice, Netbus |
| Authentication attacks (Unauthorized access) | Heartbeat (Heartbleed) | Security vulnerability in the OpenSSL cryptographic | Metasploit. SSLyze, OpenSSL, Heartbleeder, Heartbleed Honeypot |
| | Node cloning | Replicating a legal sensor node and inserting it into the network to perform illegal activities. | Rapid Clone, Not tools but used in coding, .NETInput, dojo.clone |
| Cryptographic | Brute Force | Method used to crack passwords or encryption by systematically trying all possible combinations. | Aircrack, Hydra, Medusa, Hashcat. Ncrack |
| | Side-Channel Attacks | Focusing on a system's operational or physical | ChipWhisperer, SCA toolbox, Pyecsca, Lascar, Simple Power |

(continued on next page)

**Table 6** (*continued*)

| Category of Attacks | Type of Attacks | Definition | Tools (most prevalent) |
|---|---|---|---|
| | | characteristics, including power use or electromagnetic emissions, for gathering sensitive information. | Analysis (SPA) Toolkit, Rainbow |
| Botnet attacks | Mirai attack (in DoS) | Hacked IoT devices to overload a specific website or server with traffic, blocking genuine users from accessing it. | Mirai Scanner, Mirai Bot, Telnet Scanner, BusyBox, Sora |
| Cracking attacks | Password cracking | Unauthorized access to IoT devices by guessing or breaking a password. | John The Ripper, Hashcat, RainbowCrack. Ophcrack. L0phtCrack |

- **HTTP Flood:** This involves overwhelming a target server with HTTP requests. Using malware-infected devices, attackers assemble botnets to enhance the impact. HTTP flood attacks can be of two types: HTTP POST and HTTP GET.
- **ICMP Flood:** Attackers use ICMP Echo requests or ping messages to hamper network functionality, employing a rapid-fire approach to send packets without awaiting responses.
- **Jamming attack:** Attackers purposefully disrupt wireless connections among IoT devices. This is achieved by sending potent radio signals matching the frequency of targeted devices, thereby impeding their operation [66].
- **Universal Plug and Play (UPnP):** UPnP consists of networking protocols facilitating real-time interactions among IoT devices. However, the absence of robust security measures within its framework means that UPnP can facilitate amplification attacks [67].

### 6.2. Information gathering

Information gathering entails collecting data about a specific system or network to pinpoint vulnerabilities and weaknesses potentially exploitable in subsequent attacks. Reconnaissance attacks can be categorized into passive and active forms. Passive reconnaissance is characterized by collecting information on a target without engaging in detectable activities, like perusing publicly accessible data, social engineering, or passive scanning. On the other hand, active reconnaissance involves directly probing the target to uncover vulnerabilities, such as through port or vulnerability scanning [68].

- **Vulnerability Scanning:** This approach can be employed by security professionals or malicious actors to uncover vulnerabilities in a target system or network. Once identified, these vulnerabilities might pave the way for further attacks, potentially leading to unauthorized access or malware installation [15].
- **OS Fingerprinting:** This method enables an attacker to ascertain a specific device's operating system (OS). With this knowledge, they can target inherent weaknesses in the OS. OS fingerprinting can manifest as active or passive attacks. In an active approach, attackers send packets to the target, await a response, and dissect the TCP message contents. Conversely, passive attackers act like ”sniffers,” avoiding deliberate alterations or interactions with the network [69].
- **Port Scanning:** In this technique, attackers survey their target environment by dispatching packets to specific ports on a host. By analyzing the responses, they can detect vulnerabilities and determine which services—and their respective versions—are active on the host [70].
- **User-to-Root:** In this scenario, an attacker possessing limited rights on a system seeks elevated administrator privileges. This is often achieved by exploiting software or OS vulnerabilities [71].
- **Remote-to-Local:** Here, an attacker seizes control of a remote system or network. Leveraging this control, they target a local system—like a workstation or server—by exploiting vulnerabilities in the communication protocols or connection software [71].
- **Sybil Attack:** In this approach, a malicious node purports to have multiple identities either by impersonating legitimate nodes or fabricating new, fictitious identities. The attacker might present all the Sybil identities concurrently or sequentially. Systems like routing protocols or voting-based fault tolerance mechanisms can fall prey to Sybil attacks [72].

### 6.3. Man-in-the-middle attack

A Man-In-The-Middle (MITM) attack occurs when an adversary intercepts communications between two parties, enabling them to covertly eavesdrop, modify, or inject data into the communication. Prominent MITM attacks encompass techniques such as Address Resolution Protocol (ARP) cache poisoning, Domain Name System (DNS) attacks, session theft, ICMP redirection, and port snatching [73].

- **DNS Spoofing**: This involves poisoning the DNS server records, leading a user to a malicious site controlled by the attacker. Such attacks exploit the DNS protocol's vulnerabilities and how domain name servers use the protocol [74]. Notable types of DNS spoofing include:
  - **DNS Cache Poisoning**: The attacker introduces fraudulent DNS data into the server's cache to mislead users [75].
  - **DNS ID Spoofing**: The attacker manipulates the DNS transaction ID to send deceptive DNS responses to the target server [39].
- **ARP Spoofing**: The attacker broadcasts counterfeit ARP messages over a local area network. This maps the attacker's MAC address to the IP of another host on the network, causing the network data to be redirected to the attacker's machine [76].

### 6.4. Injection attacks

An injection attack introduces malicious input data into applications from the client side. Prominent examples include Cross-site Scripting (XSS), SQL Injection, Uploading Attack, and Buffer Overflow.

- **Cross-site Scripting (XSS)**: In IoT applications, attackers often attempt to run harmful commands on a Web server. They insert malicious web content using XSS, such as rogue HTTP or JavaScript codes. This vulnerability can leak data, authentication mechanisms, session tokens, and cookies between IoT devices and remote Web servers [77].
- **SQL Injection**: Attackers exploit vulnerabilities in database-driven applications. By inserting malicious SQL commands into input fields, they can modify or exfiltrate data from the app's database.
- **Uploading Attack**: Attackers exploit vulnerabilities in web applications to upload files containing malevolent code (e.g., web shells) to a web server. Once uploaded, they can execute this code to gain unauthorized access, pilfer sensitive data, modify or delete files, or inflict other damages. These attacks might be manual or automated [78].
- **Buffer Overflow**: This happens when excessive data is written into a buffer without proper validation or boundary checks in a sensor node. The overflowing data can overwrite adjacent memory spaces, corrupting the stored data [79].

### 6.5. Malware attacks

Malware attacks represent a prevalent type of cyberattack, where

malicious software executes unauthorized actions on a victim's system. Malware can propagate through multiple mediums, such as email attachments, malevolent web pages, and compromised software. Upon penetration, malware can undertake various harmful activities, including credential theft, data encryption, or complete system takeover [80]. Examples of malware include backdoors, viruses, Trojan horses, ransomware, and adware.

- **Ransomware:** A refined type of malware that restricts access to systems or services, making them inaccessible to users until a ransom is paid. The attackers typically communicate their demands to the victim, promising to restore access to the system or provide the decryption key for the ransom [81].
- **Backdoor:** This is when an attacker exploits a vulnerability or injects malicious code into a system or network to gain unauthorized access and control. Utilizing system vulnerabilities, this software grants intruders unrestricted remote access to a breached device [82]. With this access, an attacker can eavesdrop on users, control their sessions, target other systems, install additional software, or monitor the entire network.
- **Spyware:** Unauthorized software installed on IoT devices to surreptitiously gather data. Through monitoring user activities, attackers aim to harvest confidential information using this method [83].
- **Worms:** These malicious programs replicate themselves on an IoT device and can propagate to other devices. They can inflict various damages, such as file deletion, data theft, or even full system compromise.
- **Trojan horses:** A deceptive form of malware masquerading as legitimate software. Once activated, it gives the attacker the same privileges as a regular user, enabling activities like file transfers, data edits, deletions, or altering device content [84]. Attackers often initiate Trojan horse attacks on IoT devices by camouflaging the malware as a legitimate application or driver and then persuading the user to install it.

### 6.6. Authentication attacks

Authentication attacks involve malicious entities seeking unauthorized access to a system or network. This often entails exploiting vulnerabilities in security measures or acquiring valid login credentials. Once this unauthorized access is achieved, the attacker can engage in various malicious activities such as stealing sensitive data, altering system configurations, introducing malicious software, or launching subsequent attacks within the IoT ecosystem [85].

- **Heartbleed:** In 2014, a vulnerability dubbed “Heartbleed” was discovered in the OpenSSL encryption software library. This vulnerability, specifically in the library's implementation of the Transport Layer Security (TLS) heartbeat extension, allows attackers to access sensitive data from machines running the affected OpenSSL versions, such as user passwords [86].
- **Node cloning:** A vast majority of IoT devices, ranging from sensor nodes to CCTV cameras, lack hardware tamper-proofing, primarily due to a void in standardization for IoT device designs. Consequently, these devices can easily be replicated or mimicked for malicious objectives. Attackers can replace genuine nodes with these clones through various methods, like acquiring cryptographic keys or compromising the device's firmware [87].

### 6.7. Cryptographic attacks

- **Brute Force:** This type of attack involves systematically trying every possible password or passcode combination to gain access to a system. Eventually, the attacker determines the correct credential and gains access [88].
- **Side-Channel Attacks:** These attacks exploit information gathered from the side channels of encryption devices, such as data related to the device's processing time or power consumption during encryption and decryption processes. This can also include information collected while computing various cryptographic protocols like the Diffie Hellman (DH) key exchange or the Digital Signature Standard (DSS) [89].

### 6.8. Botnet attacks

Botnets refer to networks of compromised devices controlled by an attacker. These networks can be leveraged to launch large-scale attacks, such as disseminating spam emails for financial benefits or orchestrating DDoS attacks on critical infrastructures or websites to render them dysfunctional [90].

- **Mirai attack:** Discovered in 2016, the Mirai botnet has been associated with some of the most notorious DDoS attacks. It utilizes a vast network of hijacked IoT devices, including routers, cameras, and DVRs, to flood a target website or server with overwhelming traffic, making it inaccessible to genuine users [91].
- **Password cracking:** This method involves guessing or breaking a password to gain unauthorized access to an IoT device. It generally employs automated tools or software to attempt different passwords until the correct one is identified repetitively [92].

### 6.9. Physical/backdoor attacks

A physical or backdoor attack involves gaining direct access to computer hardware, devices, or systems to exploit vulnerabilities, bypass authentication, or tamper with device operations. This type of attack contrasts with remote cyberattacks that are executed over networks. In IoT devices, physical access allows attackers to exploit interfaces and ports primarily designed for debugging, testing, or other benign purposes.

JTAG is a common interface for debugging and testing integrated circuits [93]. Given their diversity and need for testing during development, IoT devices often incorporate JTAG interfaces. However, if these interfaces are not secured post-development, they provide a potential backdoor. Attackers with physical access can connect to the JTAG interface to Ref. [94].

- **Extract Sensitive Information:** This can include cryptographic keys, personal data, or proprietary software.
- **Modify Device Functionality:** They can alter the firmware, change device settings, or install malicious code.
- **Disrupt Service:** An attacker can render a device nonfunctional or perform actions leading to malfunctioning.

From an IDS perspective, addressing physical or backdoor vulnerabilities requires [95].

- **Physical Security:** Strengthen the physical security around devices.
- **Disable Debug Interfaces:** Ensure interfaces such as JTAG are disabled post-development.
- **Hardware-based IDS:** Implement IDS solutions that monitor hardware-level operations.
- **Integrate with SIEM:** Incorporate IDS alerts into a Security information and event management (SIEM) system.
- **Regular Audits:** Periodically audit devices for vulnerabilities.

## 7. Observations, challenges, and future directions

The surge in IoT adoption has integrated it seamlessly into our daily lives due to its adaptability in catering to diverse user needs. Yet, this proliferation of IoT devices has simultaneously attracted malicious actors

aiming to compromise systems by pilfering user credentials or initiating various attacks [96].

Deep Learning (DL) techniques are typically preferred for extensive datasets, as labeling is labor-intensive and expensive. Nonetheless, the inherent depth of DL methodologies, when coupled with sizable datasets for Intrusion Detection Systems (IDS), demands substantial computational power and extended processing times [97]. It was observed that a notable fraction of the presented solutions assessed their models utilizing obsolete datasets, such as KDD Cup'99 and NSL-KDD. While some solutions demonstrated commendable outcomes on these archaic datasets, their efficacy dwindled on contemporary, more refined datasets [98]. A recurring limitation across most methods is their subpar detection of attacks, especially when presented with minimal samples during training. The challenge of class imbalances further exacerbates the situation, undermining underrepresented attack classes' accuracy and detection prowess. This imbalance issue necessitates rigorous exploration [98].

A discernible trade-off is witnessed between the model's intricacy and the profound architecture of DL methods: a deeper method invariably implies a more intricate model, with increased demands on time and computational resources. Several strategies, including transfer learning, federated learning, and edge computing, have been advocated to mitigate these hurdles. However, no singular approach has emerged as a panacea [99]. Yet, DL-infused IDS continues to be a buzzing research domain, with myriad initiatives striving to enhance their capability while circumventing inherent constraints.

Anticipated future trajectories encompass formulating more streamlined DL models trainable on condensed datasets, an amalgamation of DL with alternative security paradigms such as Blockchain and Federated Learning, and pioneering techniques to thwart adversarial intrusions [100].

## 8. Conclusion

The ubiquity of IoT devices has seamlessly integrated into our daily routines, enriching connectivity and convenience. Nevertheless, the exponential growth of IoT devices introduces pressing security challenges that must be tackled to ensure the resilience and trustworthiness of these interconnected ecosystems. This paper is structured into six sections, each elucidating the potential of Deep Learning in fortifying IoT security. Deep Learning leverages vast datasets to train intricate models, consistently outperforming other classification task techniques. Given the volatile nature of IoT, Deep Learning emerges as a superior choice for intrusion detection systems. This review presents an exhaustive exploration of diverse models suggested for IoT intrusion detection, detailing the specific challenges they aim to solve and shedding light on their efficacy.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References


[1] J.-H. Lee, H. Kim, Security and privacy challenges in the internet of things [security and privacy matters], IEEE Consumer Electronics Magazine 6 (3) (2017) 134–136.

[2] M.S. Eddine, M.A. Ferrag, O. Friha, L. Maglaras, Easbf: an efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles, J. Inf. Secur. Appl. 59 (2021) 102802.

[3] M.S. Virat, S. Bindu, B. Aishwarya, B. Dhanush, M.R. Kounte, Security and privacy challenges in internet of things, in: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). Plus 0.5em Minus 0.4emIEEE, 2018, pp. 454–460.

[4] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal, M.L.M. Kiah, A review of smart home applications based on internet of things, J. Netw. Comput. Appl. 97 (2017) 48–65.

[5] F. Panagiotis, K. Taxiarxchis, K. Georgios, L. Maglaras, M.A. Ferrag, Intrusion detection in critical infrastructures: a literature review, Smart Cities 4 (3) (2021) 1146–1157.

[6] L. Maglaras, T. Cruz, M.A. Ferrag, H. Janicke, Teaching the process of building an intrusion detection system using data from a small-scale scada testbed, Internet Technology Letters 3 (1) (2020) e132.

[7] V. Adat, B.B. Gupta, Security in internet of things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (2018) 423–441.

[8] X. Yang, L. Shu, Y. Liu, G.P. Hancke, M.A. Ferrag, K. Huang, Physical security and safety of iot equipment: a survey of recent advances and opportunities, IEEE Trans. Ind. Inf. 18 (7) (2022) 4319–4330.

[9] B. Mbarek, A. Meddeb, W.B. Jaballah, M. Mosbah, A secure authentication mechanism for resource constrained devices, in: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). Plus 0.5em Minus 0.4emIEEE, 2015, pp. 1–7.

[10] R. Fu, K. Zheng, D. Zhang, Y. Yang, An Intrusion Detection Scheme Based on Anomaly Mining in Internet of Things, IET Conference Proceedings, 2011.

[11] A. Gerodimos, L. Maglaras, M.A. Ferrag, N. Ayres, I. Kantzavelou, Iot: Communication Protocols and Security Threats, Internet of Things and Cyber-Physical Systems, 2023.

[12] M.A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, Security and privacy for green iot-based agriculture: review, blockchain solutions, and challenges, IEEE Access 8 (2020), 32 031–32 053.

[13] M.A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study, J. Inf. Secur. Appl. 50 (2020) 102419.

[14] K.A. Da Costa, J.P. Papa, C.O. Lisboa, R. Munoz, V.H.C. de Albuquerque, Internet of things: a survey on machine learning-based intrusion detection approaches, Comput. Network. 151 (2019) 147–157.

[15] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki, Network intrusion detection for IoT security based on learning techniques, IEEE Communications Surveys & Tutorials 21 (3) (2019) 2671–2701.

[16] S. Hajiheidari, K. Wakil, M. Badri, N.J. Navimipour, Intrusion detection systems in the internet of things: a comprehensive investigation, Comput. Network. 160 (2019) 165–191.

[17] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, A. Wahab, A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions, Electronics 9 (7) (2020) 1177.

[18] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, Network intrusion detection system: a systematic study of machine learning and deep learning approaches, Transactions on Emerging Telecommunications Technologies 32 (1) (2021) e4150.

[19] 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.

[20] S. Tsimenidis, T. Lagkas, K. Rantos, Deep learning in IoT intrusion detection, J. Netw. Syst. Manag. 30 (2022) 1–40.

[21] P. Jayalaxmi, R. Saha, G. Kumar, M. Conti, T.-H. Kim, Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey, IEEE Access, 2022.

[22] A. Fatani, M. Abd Elaziz, A. Dahou, M.A. Al-Qaness, S. Lu, IoT intrusion detection system using deep learning and enhanced transient search optimization, IEEE Access 9 (2021), 123 448–123 464.

[23] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, Y. Li, Data-driven intrusion detection for intelligent internet of vehicles: a deep convolutional neural network-based method, IEEE Transactions on Network Science and Engineering 7 (4) (2020) 2219–2230.

[24] I. Ullah, Q.H. Mahmoud, Design and development of A deep learning-based model for anomaly detection in IoT networks, IEEE Access 9 (2021), 103 906–103 926.

[25] W. Liang, Y. Hu, X. Zhou, Y. Pan, I. Kevin, K. Wang, Variational few-shot learning for microservice-oriented intrusion detection in distributed industrial IoT, IEEE Trans. Ind. Inf. 18 (8) (2021) 5087–5095.

[26] M.S.A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq, W.A.M. Abdullah, Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT), IEEE Access 10 (2022), 22 756–22 768.

[27] M. Zeeshan, Q. Riaz, M.A. Bilal, M.K. Shahzad, H. Jabeen, S.A. Haider, A. Rahim, Protocol-based deep intrusion detection for dos and ddos attacks using unsw-Nb15 and bot-iot data-sets, IEEE Access 10 (2021) 2269–2283.

[28] Y. Otoum, D. Liu, A. Nayak, DL-IDS: a deep learning–based intrusion detection framework for securing IoT, Transactions on Emerging Telecommunications Technologies 33 (3) (2022) e3803.

[29] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, M. Qiu, Adversarial attacks against network intrusion detection in IoT systems, IEEE Internet Things J. 8 (13) (2020), 10 327–10 335.

[30] O. Ibitoye, O. Shafiq, A. Matrawy, Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks, in: 2019 IEEE Global Communications Conference (GLOBECOM). Plus 0.5em Minus 0.4emIEEE, 2019, pp. 1–6.

[31] S.T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, R. Islam, Dependable intrusion detection system for IoT: a deep transfer learning based approach, IEEE Trans. Ind. Inf. 19 (1) (2022) 1006–1017.

[32] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, I. Kevin, K. Wang, Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system, IEEE Internet Things J. 9 (12) (2021) 9310–9319.

[33] O.A. Wahab, Intrusion detection in the iot under data and concept drifts: online deep learning approach, IEEE Internet Things J. 9 (20) (2022), 19 706–19 716.

[34] O. Alkadi, N. Moustafa, B. Turnbull, K.-K.R. Choo, A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks, IEEE Internet Things J. 8 (12) (2020) 9463–9472.
[35] F. Taher, M. Elhoseny, M.K. Hassan, I.M. El-Hasnony, A novel tunicate Swarm algorithm with hybrid deep learning enabled attack detection for secure IoT environment, IEEE Access 10 (2022), 127 192–127 204.
[36] M. Abdel-Basset, H. Hawash, R.K. Chakrabortty, M.J. Ryan, Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks, IEEE Internet Things J. 8 (15) (2021), 12 251–12 265.
[37] M.M. Alani, A.I. Awad, An intelligent two-layer intrusion detection system for the internet of things, IEEE Trans. Ind. Inf. 19 (1) (2022) 683–692.
[38] G. Thamilarasu, S. Chawla, Towards deep-learning-driven intrusion detection for the internet of things, Sensors 19 (9) (2019) 1977.
[39] Y. Zhang, P. Li, X. Wang, Intrusion detection for IoT based on improved genetic algorithm and deep belief network, IEEE Access 7 (2019), 31 711–31 722.
[40] E.M. de Elias, V.S. Carriel, G.W. De Oliveira, A.L. Dos Santos, M. Nogueira, R.H. Junior, D.M. Batista, A hybrid CNN-LSTM model for IIoT edge privacy-aware intrusion detection, in: 2022 IEEE Latin-American Conference on Communications (LATINCOM). Plus 0.5em Minus 0.4emIEEE, 2022, pp. 1–6.
[41] A. Khacha, R. Saadouni, Y. Harbi, Z. Aliouat, Hybrid deep learning-based intrusion detection system for industrial internet of things, in: 2022 5th International Symposium on Informatics and its Applications (ISIA). Plus 0.5em Minus 0.4emIEEE, 2022, pp. 1–6.
[42] A.N. Jahromi, H. Karimipour, A. Dehghantanha, An ensemble deep federated learning cyber-threat hunting model for industrial internet of things, Comput. Commun. 198 (2023) 108–116.
[43] R. Ahmad, I. Alsmadi, W. Alhamdani, L. Tawalbeh, A deep learning ensemble approach to detecting unknown network attacks, J. Inf. Secur. Appl. 67 (2022) 103196.
[44] H. Al-Hamadi, R. Chen, D.-C. Wang, M. Almashan, Attack and defense strategies for intrusion detection in autonomous distributed IoT systems, IEEE Access 8 (2020), 168 994–169 009.
[45] M. Eskandari, Z.H. Janjua, M. Vecchio, F. Antonelli, I.D.S. Passban, An intelligent anomaly-based intrusion detection system for IoT edge devices, IEEE Internet Things J. 7 (8) (2020) 6882–6897.
[46] Q. Abu Al-Haija, S. Zein-Sabatto, An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks, Electronics 9 (12) (2020) 2152.
[47] A.R. Gad, A.A. Nashat, T.M. Barkat, Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset, IEEE Access 9 (2021), 142 206–142 217.
[48] M. Shafiq, Z. Tian, A.K. Bashir, X. Du, M. Guizani, CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques, IEEE Internet Things J. 8 (5) (2020) 3242–3254.
[49] Y. Gao, J. Chen, H. Miao, B. Song, Y. Lu, W. Pan, Self-learning spatial distribution-based intrusion detection for industrial cyber-physical systems, IEEE Transactions on Computational Social Systems 9 (6) (2022) 1693–1702.
[50] L. Nie, W. Sun, S. Wang, Z. Ning, J.J. Rodrigues, Y. Wu, S. Li, Intrusion detection in green internet of things: a deep deterministic policy gradient-based algorithm, IEEE Transactions on Green Communications and Networking 5 (2) (2021) 778–788.
[51] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. Plus 0.5em Minus 0.4emIeee, 2009, pp. 1–6.
[52] N. Moustafa, J. Slay, Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set), in: 2015 Military Communications and Information Systems Conference (MilCIS). Plus 0.5em Minus 0.4emIEEE, 2015, pp. 1–6.
[53] I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating A new intrusion detection dataset and intrusion traffic characterization, ICISSp 1 (2018) 108–116.
[54] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: bot-iot dataset, Future Generat. Comput. Syst. 100 (2019) 779–796.
[55] M.-O. Pahl, F.-X. Aubet, All eyes on you: distributed multi-dimensional IoT microservice anomaly detection, in: 2018 14th International Conference on Network and Service Management (CNSM). Plus 0.5em Minus 0.4emIEEE, 2018, pp. 72–80.
[56] I. Cse-Cic-Ids2018, Cse-cic-ids2018 Dataset, 2022. https://www:unb:ca/cic/datasets/ids-2018:html.
[57] I. Sharafaldin, A.H. Lashkari, S. Hakak, A.A. Ghorbani, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: 2019 International Carnahan Conference on Security Technology (ICCST). Plus 0.5em Minus 0.4emIEEE, 2019, pp. 1–8.
[58] A. Hamza, H.H. Gharakheili, T.A. Benson, V. Sivaraman, Detecting volumetric attacks on lot devices via sdn-based monitoring of mud activity, in: Proceedings of the 2019 ACM Symposium on SDN Research, 2019, pp. 36–48.
[59] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, A. Anwar, TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems, IEEE Access 8 (2020), 165 130–165 150.
[60] I. Stratosphere Laboratory, Iot-23 Dataset, 2022. https://www.stratosphereips.org/datasets-iot23.
[61] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, Machine learning based IoT intrusion detection system: an MQTT case study (MQTT-IoT-IDS2020 dataset), in: Selected Papers from the 12th International Networking Conference: INC 2020. Plus 0.5em Minus 0, 4emSpringer, 2021, pp. 73–84.
[62] M.A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, H. Janicke, Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, IEEE Access 10 (2022), 40 281–40 306.
[63] M. Ahlmeyer, A.M. Chircu, Securing the internet of things: a review, Issues in information Systems, 17 (4) (2016).
[64] T. Sherasiya, H. Upadhyay, H.B. Patel, A survey: intrusion detection system for internet of things, Int. J. Comput. Sci. Eng. 5 (2) (2016) 91–98.
[65] S. Haris, R. Ahmad, M. Ghani, Detecting TCP SYN flood attack based on anomaly detection, in: 2010 Second International Conference on Network Applications, Protocols and Services. Plus 0.5em Minus 0.4emIEEE, 2010, pp. 240–244.
[66] I. Butun, P. Österberg, H. Song, Security of the internet of things: vulnerabilities, attacks, and countermeasures, IEEE Communications Surveys & Tutorials 22 (1) (2019) 616–644.
[67] G. Kayas, M. Hossain, J. Payton, S.R. Islam, An overview of UPnP-based IoT security: threats, vulnerabilities, and prospective solutions, in: 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Plus 0.5em Minus 0.4emIEEE, 2020, 0452–0460.
[68] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl. 84 (2017) 25–37.
[69] M.F. Elrawy, A.I. Awad, H.F. Hamed, Intrusion detection systems for iot-based smart environments: a survey, J. Cloud Comput. 7 (1) (2018) 1–20.
[70] E. Bou-Harb, M. Debbabi, C. Assi, Cyber scanning: a comprehensive survey, Ieee communications surveys & tutorials 16 (3) (2013) 1496–1519.
[71] N. Hoque, M.H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, Network attacks: taxonomy, tools and systems, J. Netw. Comput. Appl. 40 (2014) 307–324.
[72] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis & defenses, in: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 2004, pp. 259–268.
[73] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, A. Robles-Kelly, Deep learning-based intrusion detection for iot networks, in: 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC). Plus 0.5em Minus 0.4emIEEE, 2019, pp. 256–325 609.
[74] S. Raza, L. Wallgren, T. Voigt, Svelte: real-time intrusion detection in the internet of things, Ad Hoc Netw. 11 (8) (2013) 2661–2674.
[75] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, R. Atkinson, Threat analysis of iot networks using artificial neural network intrusion detection system, in: 2016 International Symposium on Networks, Computers and Communications (ISNCC). Plus 0.5em Minus 0.4emIEEE, 2016, pp. 1–6.
[76] W. Li, S. Tug, W. Meng, Y. Wang, Designing collaborative blockchained signature-based intrusion detection in iot environments, Future Generat. Comput. Syst. 96 (2019) 481–489.
[77] N. Moustafa, N. Koroniotis, M. Keshk, A.Y. Zomaya, Z. Tari, Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions, IEEE Communications Surveys & Tutorials, 2023.
[78] B. Sharma, L. Sharma, C. Lal, S. Roy, Anomaly based network intrusion detection for iot attacks using deep learning technique, Comput. Electr. Eng. 107 (2023) 108626.
[79] A.S. Dina, A. Siddique, D. Manivannan, A Deep Learning Approach for Intrusion Detection in Internet of Things Using Focal Loss Function, vol. 22, Internet of Things, 2023 100699.
[80] S.A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for ddos attacks in lightweight iot networks, Expert Syst. Appl. 215 (2023) 119330.
[81] R. Brewer, Ransomware Attacks: Detection, Prevention and Cure, Network Security, 2016, pp. 5–9, 2016.
[82] S. Hosseininoorbin, S. Layeghy, M. Sarhan, R. Jurdak, M. Portmann, Exploring edge tpu for network intrusion detection in iot, J. Parallel Distr. Comput. 179 (2023) 104712.
[83] S. Fraihat, S. Makhadmeh, M. Awad, M.A. Al-Betar, A. Al-Redhaei, Intrusion Detection System for Large-Scale Iot Netflow Networks Using Machine Learning with Modified Arithmetic Optimization Algorithm, Internet of Things, 2023 100819.
[84] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, R.M. Mohammad, Intrusion detection system using feature extraction with machine learning algorithms in iot, J. Sens. Actuator Netw. 12 (2) (2023) 29.
[85] O. Friha, M.A. Ferrag, M. Benbouzid, T. Berghout, B. Kantarci, K.-K.R. Choo, 2df-ids: decentralized and differentially private federated learning-based intrusion detection system for industrial iot, Comput. Secur. 127 (2023) 103097.
[86] A. Javadpour, P. Pinto, F. Ja'fari, W. Zhang, Dmaidps: a distributed multi-agent intrusion detection and prevention system for cloud iot environments, Cluster Comput. 26 (1) (2023) 367–384.
[87] B. Balamurugan, D. Biswas, Security in network layer of IoT: possible measures to preclude, in: Security Breaches and Threat Prevention in the Internet of Things. Plus 0.5em Minus 0, 4emIGI Global, 2017, pp. 46–75.
[88] B. Jothi, M. Pushpalatha, Wils-trs—a novel optimized deep learning based intrusion detection framework for iot networks, Personal Ubiquitous Comput. 27 (3) (2023) 1285–1301.
[89] F.-X. Standaert, Introduction to Side-Channel Attacks, Secure integrated circuits and systems, 2010, pp. 27–42.
[90] M. Jeyaselvi, R.K. Dhanaraj, M. Sathya, F.H. Memon, L. Krishnasamy, K. Dev, W. Ziyue, N.M.F. Qureshi, A highly secured intrusion detection system for iot using expso-stfa feature selection for laann to detect attacks, Cluster Comput. 26 (1) (2023) 559–574.

[91] G.-P. Fernando, A.-A.H. Brayan, A.M. Florina, C.-B. Liliana, A.-M. Héctor-Gabriel, T.-S. Reinel, Enhancing Intrusion Detection in Iot Communications through Ml Model Generalization with a New Dataset (Idsai), IEEE Access, 2023.
[92] N. Tekin, A. Acar, A. Aris, A.S. Uluagac, V.C. Gungor, Energy Consumption of On-Device Machine Learning Models for Iot Intrusion Detection, vol. 21, Internet of Things, 2023 100670.
[93] M.H. Rais, R.A. Awad, J. Lopez Jr., I. Ahmed, Jtag-based plc memory acquisition framework for industrial control systems, Forensic Sci. Int.: Digit. Invest. 37 (2021) 301196.
[94] H.A. Abdul-Ghani, D. Konstantas, A comprehensive study of security and privacy guidelines, threats, and countermeasures: an iot perspective, J. Sens. Actuator Netw. 8 (2) (2019) 22.
[95] G. Vishwakarma, W. Lee, Exploiting jtag and its mitigation in iot: a survey, Future Internet 10 (12) (2018) 121.
[96] J. Wu, H. Dai, Y. Wang, K. Ye, C. Xu, Heterogeneous Domain Adaptation for Iot Intrusion Detection: a Geometric Graph Alignment Approach, IEEE Internet of Things Journal, 2023.
[97] A. El-Ghamry, A. Darwish, A.E. Hassanien, An Optimized Cnn-Based Intrusion Detection System for Reducing Risks in Smart Farming, vol. 22, Internet of Things, 2023 100709.
[98] A. Basati, M.M. Faghih, Apae: an iot intrusion detection system using asymmetric parallel auto-encoder, Neural Comput. Appl. 35 (7) (2023) 4813–4833.
[99] T.-N. Dao, D. Van Le, X.N. Tran, Optimal network intrusion detection assignment in multi-level iot systems, Comput. Network. 232 (2023) 109846.
[100] R. Yang, H. He, Y. Xu, B. Xin, Y. Wang, Y. Qu, W. Zhang, Efficient intrusion detection toward iot networks using cloud–edge collaboration, Comput. Network. 228 (2023) 109724.