ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 13 (2024), e31919
eISSN: 2255-2863
DOI: https://doi.org/10.14201/adcaij.31919

Systematic Literature Review of Machine Learning Models for Detecting DDoS Attacks in IoT Networks

Marcos Luengo Viñuela and Jesús-Ángel Román-Gallego

Polytechnic School of Zamora, Computer Sciences Department, University of Salamanca,
Avda. Cardenal Cisneros, 34, Zamora, 49022
✉ mluevi17@usal.es, zjarg@usal.es

KEYWORDS

DDoS; IoT Networks; AI; cybersecurity; SLR; ML; Machine Learning

ABSTRACT

*The escalating integration of Internet of Things (IoT) devices has led to a surge in data generation within networks, consequently elevating the vulnerability to Distributed Denial of Service (DDoS) attacks. Detecting such attacks in IoT Networks is critical, and Machine Learning (ML) models have shown efficacy in this realm. This study conducts a systematic review of literature from 2018 to 2023, focusing on DDoS attack detection in IoT Networks using deep learning techniques. Employing the PRISMA methodology, the review identifies and evaluates studies, synthesizing key findings/2**. It highlights that incorporating deep learning significantly enhances DDoS attack detection precision and efficiency, achieving detection rates between 94 % and 99 %. Despite progress, challenges persist, such as limited training data and IoT device processing constraints with large data volumes. This review underscores the importance of addressing these challenges to improve DDoS attack detection in IoT Networks. The research's significance lies in IoT's growing importance and security concerns. It contributes by showcasing current state-of-the-art DDoS detection through deep learning while outlining persistent challenges. Recognizing deep learning's effectiveness sets the stage for refining IoT security protocols, and moreover, by identifying challenges, the research informs strategies to enhance IoT security, fostering a resilient framework.*

1. Introduction

In recent years, the widespread adoption of Internet of Things (IoT) devices has led to an explosion in the volume of data generated within networks, consequently significantly increasing the likelihood of DDoS attacks on these networks. Despite efforts to secure IoT Networks, research on novel threat detection models has progressed slowly, resulting in a gap between the evolution of attack techniques and the need for more effective detection methods.

According to a Gartner report (2021), it is anticipated that the global number of connected IoT devices will reach 41.6 billion by 2025. However, the slow evolution in threat detection model research has created a disparity between the advancement of attack techniques and the imperative for more effective detection methods. As indicated by a study by F5 Networks (Labs, 2022), 47 % of surveyed companies experienced at least one DDoS attack in 2021. This highlights the pressing need for robust DDoS attack detection mechanisms tailored to IoT Networks. However, while there exists a body of research on this topic, the evolution of threat detection models has not kept pace with the rapid advancements in attack techniques. Despite the increasing sophistication of DDoS attacks, existing detection methods often fall short in accurately and efficiently identifying and mitigating these threats in IoT environments. Hence, there is a critical need to bridge this gap by developing more effective and adaptive detection techniques.

The overarching goal of this paper is to conduct a systematic literature review on machine learning models employed for DDoS attack detection in IoT Networks. The PRISMA methodology will guide the search, selection, and analysis processes (Moher et al., 2015). Following PRISMA steps, which involve defining the research question, conducting a systematic literature search in relevant databases, applying inclusion and exclusion criteria to select pertinent studies, and analyzing results to identify the effectiveness of machine learning models and promising methodologies in DDoS attack detection in IoT Networks. Publicly available datasets for DDoS attack detection in IoT Networks have been utilized, and studies addressing the detection of a specific type of DDoS attack in IoT Networks have been included. This review also encompasses studies employing specific data preprocessing techniques for DDoS attack detection in IoT Networks. Specifically, the objectives of this research include identifying machine learning models used for DDoS attack detection in IoT Networks, analyzing the outcomes of these models, evaluating their effectiveness, identifying future challenges in DDoS attack detection in IoT Networks, and exploring opportunities to enhance detection efficacy by combining deep learning techniques with emerging technologies such as edge computing and Software-Defined Networks (SDN).

This study is justified by the imperative to develop effective techniques for DDoS attack detection in IoT Networks due to the escalating adoption of IoT devices and the substantial data generated within these networks. Additionally, addressing challenges such as insufficient training data and the limited processing capacity of IoT devices for large data volumes is essential to improve the effectiveness of DDoS IoT network attacks. The hypothesis posited is that the utilization of deep learning techniques will significantly enhance the accuracy and efficiency of DDoS attack detection in IoT Networks, as evidenced by the results obtained from the 20 selected articles in this systematic literature review.

This article is structured as follows. Section 2 presents the current state of the art; section 3 presents the methodology adopted for this review. The section on studies and their extraction is presented in section 4, and the results are discussed in section 5. Finally, section 6 presents the conclusions.

2. State of the Art

One of the widely adopted methods for detecting Distributed Denial of Service (DDoS) attacks in IoT Networks involves analyzing various types of traffic and attack vectors within network flows. This literature review explores diverse proposals for detecting malicious traffic, specifically focusing on machine learning-based detection models, particularly those employing supervised learning.

In the study by Vieira et al. (2022) various machine learning algorithms, including Decision Trees, Random Forest, Neural Networks, and Support Vector Machines, were compared for detecting distributed intrusions in IoT Networks. The CIC-IDS-2017 dataset containing attributes related to network traffic and both normal and malicious traffic, was utilized (Sharafaldin et al., 2018). Another article by ElKashlan et al. (2022) proposed a machine learning-based intrusion detection system for detecting DDoS attacks in IoT Networks, employing Neural Networks and Support Vector Machines on the DARPA 1998 dataset (Laboratory, 1998), which simulates DDoS attacks. Additionally, Awajan (2023) introduced a deep learning-based intrusion detection system for IoT Networks, utilizing Convolutional Neural Networks on the UNSW-NB15 dataset (Moustafa and Slay, 2015), containing both normal and malicious traffic.

An alternative perspective on DDoS attack detection was presented by Ali et al. (2023), providing a systematic review of machine learning algorithms used for detecting DDoS attacks in Software-Defined Networks (SDN). Various algorithms, including Decision Trees, Neural Networks, Support Vector Machines, and Random Forest, were evaluated on the CIC-IDS-2017 and NSL-KDD (Tavallaee et al., 2009) datasets, both containing normal and malicious traffic. Another SDN-oriented study by Sangodoyin et al. (2021), explored the detection and classification of DDoS flooding attacks in SDNs using Decision Trees, Random Forest, and Support Vector Machines on the NSL-KDD and DARPA 1999 datasets.

Innovative implementations include that of Khanday et al. (2023), proposing an intrusion detection model for DDoS attacks in lightweight IoT Networks using the Random Forest algorithm. The model, generated through simulation, achieves high detection rates and low false positives. Zhang et al. (2022) presented a deep learning-based method using a Bidirectional Long Short-Term Memory (BiLSTM) neural network for DDoS attack detection in edge computing networks, demonstrating effectiveness on the CIC-IDS-2017 dataset. Additionally, Farukee et al. (2021) proposed a hybrid model combining deep learning and Random Forest for DDoS attack detection in IoT Networks, achieving high precision and low false positive rates on the CIC-IDS-2017 dataset.

A comparison of various deep learning methods is presented in the article «Deep learning in distributed denial-of-service attacks detection method for internet of things networks” (Aswad et al., 2023), introducing a DDoS attack detection method for IoT Networks using Convolutional Neural Networks and Recurrent Neural Networks on the CIC-IDS-2017 dataset, with experimental results demonstrating high detection rates and low false positives.

Within the literature review domain, Wehbi et al. (2019) provided a comprehensive overview of machine learning techniques for detecting DDoS attacks in IoT systems. The authors discussed various supervised and unsupervised algorithms, such as Neural Networks, SVM, Decision Trees, and k-means, emphasizing the importance of well-designed and diverse datasets, including CIC-IDS2017, UNSW-NB15, and IoT-23, to ensure accurate and effective DDoS attack detection models.

3. Methodology

In the case of the systematic review of machine learning models for the detection of DDoS attacks in IoT Networks, the following steps of the PRISMA methodology (Moher et al., 2009) have been followed:

- **Definition of Research Questions:** This article aims to address the following research questions:
  - **RQ1:** What are the most effective machine learning models for DDoS attack detection in IoT Networks?
  - **RQ2:** How can the effectiveness of DDoS attack detection in IoT Networks be improved by combining deep learning techniques with emerging technologies?

- **Systematic Literature Search:** After verifying the absence of a recent systematic review in the literature that would answer the proposed research questions, a compilation of articles constituting the study universe has been conducted. An exhaustive search will be carried out in relevant databases (e.g., IEEE Xplore, Springer, ACM Digital Library, Scopus, etc.) using search terms related to DDoS attack detection in IoT Networks and machine learning models.

- **Systematic Search Strings** (Schardt et al., 2007):
  - **SS1:** ('DDoS' OR 'distributed denial-of-service' OR 'network attack' OR 'botnet') AND ('machine learning' OR 'deep learning' OR 'neural network' OR 'random forest') AND ('intrusion detection system' OR 'IDS' OR 'attack detection') AND ('IoT' OR 'Internet of Things' OR 'wireless sensor network' OR 'WSN')
  - **SS2:** ('DDoS' OR 'distributed denial-of-service' OR 'network attack' OR 'botnet') AND ('machine learning' OR 'deep learning' OR 'neural network' OR 'random forest') AND ('intrusion detection system' OR 'IDS' OR 'attack detection') AND ('survey' OR 'comparative analysis' OR 'systematic review')

- **Limitations:**
  - **L1:** Only articles published between 01-01-2018 and 01-03-2023 will be considered.
  - **L2:** Only articles written in English will be included.

- **Study Selection:** Inclusion and exclusion criteria will be applied to select relevant articles.
- **Inclusion Criteria:**
  - **IC1:** Studies must use machine learning models for DDoS attack detection in IoT Networks. **IC2:** Studies must present empirical results.
  - **IC3:** Studies must be written in English.
  - **IC4:** Studies must be published in scientific journals.
  - **IC5:** Studies must have been published from 2018 to the present.
  - **IC6:** Studies must use public and available datasets for DDoS attack detection in IoT Networks.
  - **IC7:** Studies that compare the effectiveness of various machine learning models for DDoS attack detection in IoT Networks.

- **IC8:** Studies that use specific data preprocessing techniques for DDoS attack detection in IoT Networks, such as normalization or dimensionality reduction.
- **IC9:** Studies that address the detection of a specific type of DDoS attack in IoT Networks, such as the SYN flood or NTP amplification attack.

- **Exclusion Criteria:**
  - **EC1:** Studies that do not use machine learning models for DDoS attack detection in IoT Networks.
  - **EC2:** Studies that do not present empirical results or lack sufficient scientific validity.
  - **EC3:** Studies not written in English or not published in scientific journals.
  - **EC4:** Studies published before 2018 or after March 2023.
  - **EC5:** Studies not focused on the detection of DDoS attacks in IoT Networks.
  - **EC6:** Studies focused on the detection of DDoS attacks in networks other than IoT.
  - **EC7:** Studies that use only unsupervised machine learning techniques for DDoS attack detection in IoT Networks.
  - **EC8:** Studies focused on the detection of DDoS attacks in a specific network topology (e.g., star network or mesh network) that is not relevant to IoT Networks.

- **Study Quality Evaluation:** The questionnaire allows to assess the quality of each considered article. This questionnaire was constructed on the basis of the information gathered during the article readings.

The utilized questionnaire is as follows:

- **P1:** Does the article address the problem of DDoS detection?
- **P2:** Does it use a dataset with NetFlow traffic flows?
- **P3:** Are Machine Learning algorithms employed?
- **P4:** Does it specify the dataset used, and is it public?
- **P5:** Is there a comparison of different machine learning models?
- **P6:** Does it propose any innovative method for DDoS attack detection?

- **Questionnaire Evaluation Criteria:** One point was assigned for each question answered with a «Yes» and a value of 0 was assigned if the answer was «No». An article can score a maximum of six points. To ensure the quality of the selected articles, the following acceptance criterion has been established:
  - **C1:** The minimum score for an article to be admitted is 4 points.

- **Data Extraction and Synthesis:** At this stage, relevant data from each selected study was extracted and synthesized into a table for ease of comparison and analysis. The machine learning models used, IoT network characteristics, types of detected DDoS attacks, and obtained results were identified. Additionally, information about authors, publication date, methodology used, key findings, and conclusions was recorded.
- **Data Analysis:** The extracted data from the selected studies was analyzed to identify common trends and patterns. The most commonly used machine learning models, IoT network

characteristics used for model training, and common types of DDoS attacks were identified. The limitations of the studies have been outlined, and the implications of the results for clinical practice and future research have been discussed.

- **Results Reporting:** At this stage, the results of the systematic review have been presented clearly and concisely, following PRISMA guidelines. The report discusses the implications of the results for practice and future research. The limitations of the included studies were identified, and recommendations for future research have been proposed. The report has been logically and coherently structured, including an introduction explaining the context and purpose of the review, a clearly described methodology, systematically presented results, and a discussion interpreting the findings.

  Concerning potential ethical issues, project limitations, and/or important considerations, the methodology defines the following aspects:

  ○ **Privacy and Confidentiality:** During the literature search and analysis, it is crucial to ensure not to disclose confidential or private information that could identify individuals or companies. If data from previous research is used, it is necessary to verify if it has been adequately anonymized.

  ○ **Environment:** Some machine learning models may require a significant amount of energy and computational resources, potentially impacting the environment. This aspect should be taken into account when selecting models and evaluating their effectiveness.

  ○ **Bias and Generalization:** The systematic literature review relies on existing studies, which may be biased and not accurately represent reality. Additionally, machine learning models may face issues of generalization and may not perform equally well in different contexts. These aspects should be considered in assessing the quality of studies and selecting machine learning models.

  ○ **Security:** Detecting DDoS attacks in IoT Networks is a critical security topic. Therefore, it is important to consider the security of the information systems used in the systematic review and the implementation of machine learning models.

  ○ **Project Limitations:** The project is limited to reviewing studies published from 2018 to the present and studies written in English. Additionally, only public and available datasets have been used for DDoS attack detection in IoT Networks. These limitations could restrict the quantity and quality of the available information and may limit the generalizability of the obtained results.

4. Study Extraction and Selection

Once the study scope has been defined, a form has been created to collect relevant data from each article based on the research questions formulated in the methodology section. Data have been extracted from a thorough reading of each article, and variables have been chosen for measurement to ensure systematic, objective, and reproducible review.

4.1. The Variables to Be Extracted

Firstly, the choice of datasets (V1) reflects the evolving nature of threats, with each dataset created at different times, capturing the changing patterns of attack behavior. Secondly, the type of targeted

DDoS attacks (V2) varies widely, encompassing packet flooding attacks, distributed denial-of-service attacks, and others, highlighting the breadth of security concerns faced by IoT Networks. This diversity extends to the machine learning algorithms employed (V3), ranging from traditional approaches such as KNN to more sophisticated models such as CNN and LSTM, showcasing the versatility in approach. Despite these differences, many studies achieve high accuracy rates (V4) in detection, with some surpassing 99 %, underscoring the effectiveness of machine learning models in identifying malicious activity. However, disparities in computational efficiency (V5) emerge, with training and classification times varying significantly, suggesting potential challenges in scalability. To mitigate these issues, various data preprocessing techniques (V6), including feature selection and normalization, are utilized to enhance model accuracy, emphasizing the importance of optimizing performance through effective data preparation.

4.2. Data Extraction and Selection Diagram

1. Following the systematic search for articles using logical expressions SE1 and SE2, 60 articles were found across IEEE Digital Library, Scopus, Science Direct, MDPI, and Springer.
2. In the initial deduplication, 5 articles were removed due to content duplications, leaving 55 articles for the application of inclusion and exclusion criteria defined in the next section.
3. The application of the inclusion criteria, following the PRISMA methodology, resulted in a total of 25 articles. A total of 30 exclusions were due to publication date and the unavailability of public datasets. When applying exclusion criteria, 8 more articles were excluded due to the non-relevance of the examined attacks or the use of outdated technologies. Thus, after these two filters, a set of 17 articles was obtained.
4. As shown in Figure 1 and detailed in the previous section, a 7-point questionnaire was applied, scoring the relevance of each article. Based on the established minimum score, 4 more articles were discarded, resulting in a set of only 13 articles.
5. The final filtering was done due to the initial condition of having a reduced literature set of only 10 articles. Based on the previous scoring criterion, articles with greater relevance for the literature review were selected, excluding from the revision 3 more articles.
6. Once these 10 articles were grouped, data from each of them was extracted to answer the research question posed, focusing especially on the datasets and algorithms used.

It is essential to note that the results obtained from the analyzed algorithms depend on the datasets to which they are applied.

4.3. Table for Systematic Literature Review

Based on the previously identified variables, a review of the reviewed articles has been generated for subsequent analysis and conclusion extraction.

Table 1 consists of references to articles extracted from the detailed process in the PRISMA diagram, the dataset used for experimentation, machine learning algorithms employed, accuracy metrics obtained, training time employed, and another column for any applied data preprocessing. Based on these variables, the following comparative systematic review is proposed.

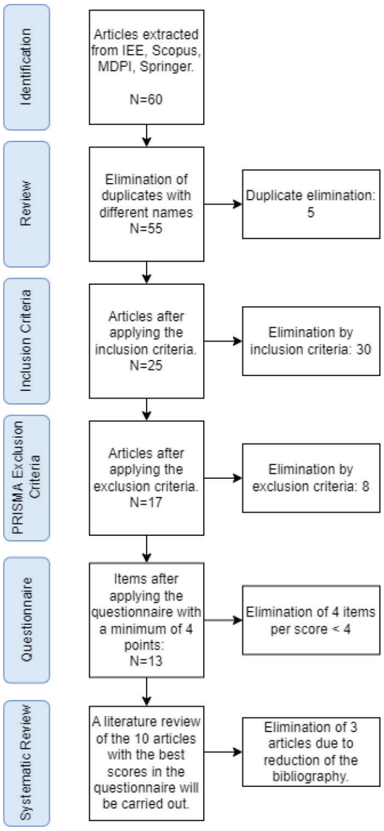
Identification
Articles extracted from IEE, Scopus, MDPI, Springer.
N=60
Review
Elimination of duplicates with different names
N=55
Duplicate elimination: 5
Inclusion Criteria
Articles after applying the inclusion criteria.
N=25
Elimination by inclusion criteria: 30
PRISMA Exclusion Criteria
Articles after applying the exclusion criteria.
N=17
Elimination by exclusion criteria: 8
Questionnaire
Items after applying the questionnaire with a minimum of 4 points:
N=13
Elimination of 4 items per score < 4
Systematic Review
A literature review of the 10 articles with the best scores in the questionnaire will be carried out.
Elimination of 3 articles due to reduction of the bibliography.

Figure 1. Prisma diagram for article extraction and selection

Table 1. Comparative table for systematic review of defined study variables

Article	Dataset	Attack Type	ML Algorithm	Accuracy	Training Time	Preprocessing
(Vieira et al., 2022)	MQTT-IoT-IDS2020 (MQTT)	Mixed IDS	KNN	99.974 %	4 ms	Feature
(Vieira et al., 2022)	MQTT-IoT-IDS2020 (MQTT)	Mixed IDS	RF	99.952 %	3 ms	Selecting
(Vieira et al., 2022)	MQTT-IoT-IDS2020 (COAP)	Mixed IDS	DT	99.904 %	2 ms	One-Hot
(Vieira et al., 2022)	MQTT-IoT-IDS2020 (COAP)	Mixed IDS	RF	99.732 %	4 ms	Encoding
(ElKashlan et al., 2022)	IoT-23	Mixed	Decision Table	99.99 %	61.6 s	Attribute selection

(continued)

Table 1. Comparative table for systematic review of defined study variables (continued)

Article	**Dataset**	**Attack Type**	**ML Algorithm**	**Accuracy**	**Training Time**	**Preprocessing**
(ElKashlan et al., 2022)	IoT-23	Mixed	Filtered Classifier	99.97 %	75 ms	Attribute selection
(Awajan, 2023)	WUSTL-IIOT-2021	Mixed	Deep Intrusion Detection (DID)	95.1 %	-	Normalization and One-Hot encoding
(Ali et al., 2023)	CICIDS2017	Mixed IDS	CNN	99.96 %	- s	Dropout 0.5
(Ali et al., 2023)	CICIDS2017	Mixed IDS	AE-SVM	99.97 %	15.31 s	-
(Ali et al., 2023)	CICDDoS2019	DDoS	Resnet-CNN	99.98 %	- s	-
(Ali et al., 2023)	CICDDoS2019	DDoS	LSTM	99.97 %	- s	Feature Hashing and Bag of Words
(Sangodoyin et al., 2021)	SDNDDoS2021	DDoS	CART	98.7 %	12.4 ms	Segmentation and One-Hot encoding
(Khanday et al., 2023)	BOTIoT2018	DDoS	Linear SVM	99.0 %	12.4 ms	Normalization and Standardization
(Khanday et al., 2023)	TONIoT2020	DDoS	LSTM	99.97 %	- s	Normalization and Standardization
(Zhang et al., 2022)	Public Datasets	DDoS	BiLSTM	95.96 %	- ms	Time-Series Extraction
(Farukee et al., 2021)	CICIDS2017	DDoS	RF-MLP	99.58 %	- ms	Remove IP
(Farukee et al., 2021)	CICIDS2017	DDoS	RF-CNN	99.63 %	- s	MinMax Normalization
(Aswad et al., 2023)	CICIDS2017	DDoS	CNN-BiLSTM	99.76 %	- ms	Label Encoding
(Wehbi et al., 2019)	ISCX2012	DDoS	KNN	99.99 %	High	Hadoop Distributed File System

4.4. Explanation of Comparative from Table 1 for Systematic Literature Review

The comparative analysis between the defined study variables and Table 1 reveals a consistent alignment in methodologies and outcomes. The diverse range of datasets utilized in the reviewed articles reflects the evolving nature of threats in IoT Networks (V1), while the targeted DDoS attack types encompass a broad spectrum of security concerns (V2). Similarly, the versatility of the employed machine learning algorithms mirrors the diverse approaches outlined in the study variables (V3), with high accuracy rates consistently exceeding 99 % (V4). Disparities in computational efficiency, evident in varying training times, echo potential scalability challenges highlighted in the study variables (V5).

Moreover, the application of various data preprocessing techniques, such as feature selection and normalization, underscores the emphasis on optimizing model performance through effective data preparation (V6). This congruence underscores the relevance of the defined study variables in understanding and evaluating state-of-the-art approaches to DDoS attack detection in IoT Networks.

In relation to the comparability of experimental results in Table 1, it is evident that the diversity in datasets, preprocessing techniques, and machine learning algorithms used among the reviewed studies poses challenges for direct comparison. For example, the studies by Vieira et al. (2022) employed different datasets (MQTT-IoT-IDS2020 MQTT vs. MQTT-IoT-IDS2020 COAP) and preprocessing techniques (Feature vs. Selecting vs. One-Hot vs. Encoding), making it difficult to generalize the results. Additionally, variability in sample size and class imbalance, as observed in datasets CICDDoS2019 and SDNDDoS2021, may influence the comparison of model accuracy. Therefore, caution should be exercised when interpreting the results and careful consideration should be given to contextual differences among studies before drawing definitive conclusions.

Regarding the statistical significance of differences in error rates among the analyzed strategies in Table 1, while error rates may appear comparatively similar, it is essential to conduct appropriate statistical tests to determine if the differences are statistically significant. For example, when comparing the results of CNN, AE-SVM, and Resnet-CNN models by Ali et al. (2023) on the CICIDS2017 dataset, an analysis of variance (ANOVA) followed by post hoc tests could be performed to assess the significance of differences. Additionally, to determine if deep learning or hybrid methods are significantly superior to techniques such as Random Forest or SVM, hypothesis testing, such as the Student’s t-test, can be employed with a predefined significance level. However, it is important to note that the efficacy of a particular approach may depend on various factors, such as problem complexity and data availability, and there is no one-size-fits-all solution. Therefore, a comprehensive evaluation of different approaches based on specific problem needs and computational limitations is recommended.

While the analysis of result comparability and the evaluation of statistical significance are important aspects of research, these questions may require additional studies and specific analyses beyond the scope of this work. Therefore, future research is recommended to focus on addressing these issues in a more detailed and specific manner.

5. Results and Discussion

In this section, we present the results and discussions derived from the systematic literature review conducted on the topic of DDoS attack detection in IoT Networks using machine learning techniques. The analysis encompasses several key aspects, including the impact of the reviewed literature, characteristics of the datasets employed in various approaches, and the balance of data classes within these datasets.

5.1. Analysis of the Impact of the Reviewed Literature

After conducting the analysis of the articles extracted in the systematic literature review process, the impact of the different extracted articles meeting the inclusion and exclusion criteria has been assessed and reflected in Table 2.

To perform the analysis, the following equation definitions have been employed.

Citation Index:

$$IC_a = \frac{\sum_{i=1}^{n} C_i}{n} \tag{1}$$

Where:

a. *ICa* is the citation index of article *a*.
b. *ci* is the number of citations received by article *a* in year *i*.
c. *n* is the number of years evaluated.

Impact Factor:

$$FI_j = \frac{A_j}{C_j} \tag{2}$$

Where:

d. *FIj* is the impact factor of journal *j*.
e. *Cj* is the total number of citations received by articles published in journal *j* in the previous year.
f. *Aj* is the total number of articles published in journal *j* in the previous year.

5.2. Database Indexing

It is a qualitative measure indicating the database in which the article is indexed. Depending on the relevance of the journal, the article may have greater scientific rigor and impact.

Table 2. Comparative table of the impact of articles on DDoS attack detection in IoT using machine learning techniques

Reference	**Impact Factor**	**Citations**	**Indexing**
(Gartner, 2021)	0.969	1	Scopus
(Labs, 2022)	3.54	65	IEEE Xplore
(Vieira et al., 2022)	2.217	131	ESCI, Scopus
(ElKashlan et al., 2022)	3.275	40	ESCI, Scopus
(Awajan, 2023)	3.745	15	IEEE Xplore
(Ali et al., 2023)	5.452	22	SCI, Scopus
(Sangodoyin et al., 2021)	3.057	21	ESCI, Scopus
(Khanday et al., 2023)	3.638	6	Scopus
(Zhang et al., 2022)	1.607	4	ESCI, Scopus
(Farukee et al., 2021)	0.268	24	IEEE Xplore

As shown in Table 2, and based on the obtained Impact Factor results, it can be determined that the article with the highest impact is that of Khanday et al. (2023), where authors proposed an intrusion detection model for DDoS attacks in lightweight IoT Networks using supervised algorithms such as SVM and LSTM to achieve the best detection results on TON-IoT and BoT-IoT datasets.

5.3. Analysis of Dataset Characteristics

After concluding the analysis of the training datasets used in different approaches to DDoS attack detection, the number of features has been compiled, and the original dataset sources are referenced in Table 3. Additionally, a more in-depth analysis has been performed in Table 4 on the number of samples and the balance of data classes to determine which datasets have greater potential for use in future research.

Table 3. Table with data from different datasets, number of features, and references to the original data sources

Dataset	**Year**	**Number of Features**	**Reference**
MQTT-IoT-IDS2020	2020	82	(Alrawashdeh et al., 2020)
IoT-23	2020	1 152	(Alaba et al., 2021)
WUSTL-IIOT-2021	2021	41	(Jain, 2021)
CICIDS2017	2017	78	(Shiravi et al., 2012)
CICDDoS2019	2021	86	(Alshammari and Zincir-Heywood, 2020)
BOTIoT2018	2018	49	(Kolias et al., 2018)
TONIoT2020	2020	9	(Ramos et al., 2020)
SDNDDoS2021	2021	23	(Sangodoyin et al., 2021)

The balance of data is particularly relevant during the training of machine learning models, which is why Table 4 reflects the distribution of different datasets and the number of samples present in each.

Table 4. Table with datasets, distribution of benign and malicious data in two columns, and data collection type

Dataset	**Samples**	**Normal**	**Malicious**	**Type**
MQTT-IoT-IDS2020	25,633	51 %	49 %	Simulated
IoT-23	42,293	55 %	45 %	Simulated (Cooja)
WUSTL-IIOT-2021	1 194.464	92.72 %	7.28 %	Simulated
CICIDS2017	2 830.743	60 %	40 %	Simulated
CICDDoS2019	51 427.365	0 %	100 %	Scanned
ISCX2012	2 450.000	56.78 %	43.22 %	Simulated
NSL-KDD	125.973	73.6 %	26.4 %	Simulated
KDDCUP99	4 898.431	99.7 %	0.3 %	Scanned
BOTIoT2018	1 246.312	57.32 %	42.68 %	Simulated
TONIoT2020	20.000	97.96 %	2.04 %	Simulated
SDNDDoS2021	3.600	0 %	100 %	Scanned

5.4. In-Depth Analysis of Research Approaches

In this section, we provide a comprehensive examination of the strengths and limitations of the diverse research lines analyzed, aiming to justify the most effective approaches for detecting attacks in IoT Networks.

Firstly, we scrutinize the performance of machine learning algorithms employed across studies, considering factors such as accuracy, computational efficiency, and scalability (Table 1). While deep learning methods such as CNN and LSTM showcase impressive accuracy rates, their computational demands may hinder real-time deployment, whereas traditional algorithms such as KNN offer faster processing but may sacrifice detection accuracy. Additionally, we explore the impact of data preprocessing techniques on model performance, highlighting the role of feature selection, normalization, and encoding methods in enhancing detection efficacy (Table 2). Despite their effectiveness, these techniques often require domain expertise and may introduce biases if not applied judiciously. Furthermore, we delve into the diversity of DDoS attack types targeted in each study, recognizing the need for models capable of detecting various attack vectors (Table 3). While some studies focus on specific attack types for depth, others adopt a broader approach, balancing between specialization and generalizability.

Finally, we assess the suitability of the datasets utilized, considering factors such as size, diversity, and class balance (Table 4). Datasets with balanced class distributions and realistic representations of IoT network traffic are deemed more suitable for training robust detection models. By critically analyzing these aspects, we aim to elucidate the most effective research directions for advancing DDoS attack detection in IoT Networks, emphasizing the importance of methodological rigor, scalability, and dataset quality in driving meaningful progress in the field.

6. Conclusions

The security of IoT is a rapidly evolving field, and the availability of quality datasets is crucial for research in this domain. The presented tables provide valuable information about some of the most commonly used datasets in the IoT security research community, which can be beneficial for those exploring this research area. The obtained results reveal several datasets commonly used for machine learning model training, such as the CICDDoS2019 dataset and the CICIDS2017 dataset. In Table 1, various machine learning algorithms have been compared, and it is found that decision tree-based algorithms, such as Random Forest, SVM, and DT, yield good results in detecting DDoS attacks in IoT Networks. It is also concluded that neural network-based algorithms, such as RF-MLP and RF-CNN, perform well in this context.

The comparative table of the systematic review (Table 1) of Machine Learning models for DDoS attack detection in IoT Networks is a useful tool for synthesizing and comparing the results of different reviewed studies. As observed, various aspects were evaluated, including the dataset used, the type of attack, the machine learning algorithm employed, accuracy, training time, and data preprocessing. Overall, studies utilize different datasets and preprocessing techniques, making a direct comparison of the results challenging. However, most studies achieve high accuracy in detecting DDoS attacks in IoT Networks, with accuracy values ranging between 95.1 % and 99.99 %. The most used algorithms were KNN, RF, and LSTM, while common preprocessing techniques included normalization, standardization, and one-hot encoding.

In conclusion, this review study has demonstrated the importance of datasets in intrusion detection research on the Internet of Things. Various dataset characteristics, such as size, data type, number of features, data collection type, among others, have been identified and analyzed. It is also noted that there is significant variability in the distribution of benign and malicious data in different datasets.

This study underscores the need to continue improving the quality and quantity of datasets used in IoT intrusion detection research. More efforts are required to develop realistic and representative datasets that encompass a wide variety of devices, network topologies, and attack scenarios. Furthermore, additional studies are needed on the evaluation and comparison of different intrusion detection techniques using diverse datasets and evaluation metrics.

Regarding future research directions, several avenues can be explored. For instance, work can be done on the development of new dataset generation techniques, allowing for the creation of more realistic and representative datasets. Investigation into knowledge transfer between different datasets, i.e., how intrusion detection techniques trained on one dataset can be used to enhance detection on another dataset, is another potential avenue. Additionally, research can be conducted on new evaluation metrics for intrusion detection techniques, considering aspects such as the robustness and scalability of the techniques, as well as the application of these techniques in SDN, edge computing, or other innovative methods to enhance the overall performance of the studied methods.

Funding

It should be noted that this initiative is carried out within the framework of the Recovery, Transformation and Resilience Plan funds, financed by the European Union (Next Generation).

Abbreviations

This article employs the abbreviations listed in Table 5.

Table 5. Abbreviations

Abbreviation	Meaning
DDoS	Distributed Denial of Service
IoT	Internet of Things
SDN	Software Defined Network
SLR	Systematic Literature Review
ML	Machine Learning
LSTM	Long-Short Term Memory
CNN	Convolutional Neural Network
CE	Exclusion Criteria
CI	Inclusion Criteria
DNN	Deep Neural Networks
DT	Decision Tree

(continued)

Table 5. Abbreviations (continued)

Abbreviation	**Meaning**
IDS	Intrusion Detection System
IP	Internet Protocol
KNN	K-Nearest Neighbors
LR	Logistic Regression
NB	Naive Bayes
SVM	Support Vector Machines
AI	Artificial Intelligence

References

Alaba, F., Hammoudeh, M., & Newman, R. (2021). IoT-23: A dataset of 23 IoT devices for intrusion detection. En *2021 7th International Conference on Information Management (ICIM)* (pp. 56–63). IEEE.

Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Applied Sciences, 13*(5). https://doi.org/10.3390/app13053183

Alrawashdeh, S., Hossain, M. S., & Al-Dmour, H. (2020). MQTT-IoT-IDS2020: A dataset for evaluating the performance of intrusion detection systems in IoT MQTT environments. *Zenodo*. https://doi.org/10.5281/zenodo.4449822

Alshammari, R., & Zincir-Heywood, A. N. (2020). CICDDoS2019: A new dataset for DDoS attacks and normal traffic. En *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 157–165). IEEE.

Aswad, F. M., Ahmed, A. M. S., Alhammadi, N. A. M., Khalaf, B. A., & Mostafa, S. A. (2023). Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. *Journal of Intelligent Systems, 32*(1), 20220155. https://doi.org/10.1515/jisys-2022-0155

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT Networks. *Computers, 12*(2). https://doi.org/10.3390/computers12020034

ElKashlan, M., Aslan, H., & Azer, M. (2022). DDoS attack detection in IoT using machine learning-based intrusion detection system (IDS). *IEEE Explore*, 19–24. https://doi.org/10.1109/ICENCO55801.2022.10032515

Farukee, M. B., Shabit, M. S. Z., Haque, M. R., & Sattar, A. H. M. S. (2021). DDoS attack detection in IoT Networks using deep learning models combined with random forest as feature selector. In M. Anbar, N. Abdullah, & S. Manickam (Eds.), *Advances in Cyber Security. ACeS 2020. Communications in Computer and Information Science* (vol. 1347, pp. 118–134). Springer, Singapore. https://doi.org/10.1007/978-981-33-6835-4_8

Gartner. (2021). *Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2021*.

Jain, R. (2021). *WUSTL-IIOT-2021 dataset*. https://www.cse.wustl.edu/~jain/iiot2/index.html

Khanday, S. A., Fatima, H., & Rakesh, N. (2023). Implementation of intrusion detection model for DDoS attacks in lightweight IoT Networks. *Expert Systems with Applications, 215*, 119330. https://doi.org/10.1016/j.eswa.2022.119330

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2018). BoT-IoT: A dataset for IoT botnet attacks.

Laboratory, L. (1998). *1998 DARPA intrusion detection evaluation dataset*.

Labs, F. (2022). *2022 application protection report: In expectation of exfiltration*.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine, 151*(4), 264–269. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L. A., & PRISMA-P Group. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews, 4*, 1–9. https://doi.org/10.1186/2046-4053-4-1

Moustafa, N., & Slay, J. (2015). 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)* (pp. 1–6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942

Ramos, D., Marin, J. M., de Goyeneche, J.-M., & Lopez, D. R. (2020). TON-IoT: A novel dataset for building IoT intrusion detection systems.

Sangodoyin, A. O., Akinsolu, M. O., Pillai, P., & Grout, V. (2021). Detection and classification of DDoS flooding attacks on software-defined networks: A case study for the application of machine learning. *IEEE Access, 9*, 122495–122508. https://doi.org/10.1109/ACCESS.2021.3109490

Schardt, C., Adams, M. B., Owens, T., Keitz, S., & Fontelo, P. (2007). Utilization of the PICO framework to improve searching PubMed for clinical questions. *BMC Medical Informatics and Decision Making, 7*(1). https://doi.org/10.1186/1472-6947-7-16

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP, 1*, 108–116. https://doi.org/10.5220/0006639801080116

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security, 31*(3), 357–374. https://doi.org/10.1016/j.cose.2011.12.012

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. En *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1–6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528

Vieira, M. N., Oliveira, L. P., & Carneiro, L. (2022). A comparative analysis of machine learning algorithms for distributed intrusion detection in IoT Networks. En *Springer International Publishing* (pp. 249–258). https://doi.org/10.1007/978-3-030-99584-3_22

Wehbi, K., Hong, L., Al-salah, T., & Bhutta, A. A. (2019). A survey on machine learning-based detection on DDoS attacks for IoT systems. *IEEE Explore*, 1–6. https://doi.org/10.1109/SoutheastCon42311.2019.9020468

Zhang, Y., Liu, Y., Guo, X., Liu, Z., Zhang, X., & Liang, K. (2022). A BiLSTM-based DDoS attack detection method for edge computing. *Energies, 15*(21). https://doi.org/10.3390/en15217882