KeAi
CHINESE ROOTS
GLOBAL IMPACT

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

A survey on intrusion detection system in IoT networks

Md Mahbubur Rahman[a], Shaharia Al Shakil[b,*], Mizanur Rahman Mustakim[a]

[a] *Comp. Sci. & Tech., Beijing Institute of Technology, Beijing, China*
[b] *Info. & Comm. Eng., Beijing Institute of Technology, Beijing, China*

ARTICLE INFO

Keywords:
Cyber-physical systems
Distributed denial-of-service
Internet of Things
Intrusion detection
Machine learning

ABSTRACT

As the Internet of Things (IoT) expands, the security of IoT networks has becoming more critical. Intrusion Detection Systems (IDS) are essential for protecting these networks against malicious activities. Artificial intelligence, with its adaptive and self-learning capabilities, has emerged as a promising approach to enhancing intrusion detection in IoT environments. Machine learning facilitates dynamic threat identification, reduces false positives, and addresses evolving vulnerabilities. This survey provides an analysis of contemporary intrusion detection techniques, models, and their performances in IoT networks, offering insights into IDS design and implementation. It reviews data extraction techniques, useful matrices, and loss functions in IDS for IoT networks, ranking top-cited algorithms and categorizing IDS studies based on different approaches. The survey evaluates various datasets used in IoT intrusion detection, examining their attributes, benefits, and drawbacks, and emphasizes performance metrics and computational efficiency, providing insights into IDS effectiveness and practicality. Standardized evaluation metrics and real-world testing are stressed to ensure reliability. Additionally, the survey identifies significant challenges and open issues in ML and DL-based IDS for IoT networks, such as computational complexity and high false positive rates, and recommends potential research directions, emerging trends, and perspectives for future work. This forward-looking perspective aids in shaping the future direction of research in this dynamic field, emphasizing the need for lightweight, efficient IDS models suitable for resource- constrained IoT devices and the importance of comprehensive, representative datasets.

1. Introduction

The Internet of Things (IoT) is a worldview that empowers the interconnection and communication of different physical and virtual gadgets through the Web. IoT networks serve several domains, including smart cities, health, agriculture, and transportation. In any case, IoT networks additionally face numerous security challenges, like unapproved access, information theft, denial of service, and malicious attacks. Accordingly, it is fundamental to plan and execute compelling intrusion detection systems (IDS) for IoT organizations to safeguard them from likely dangers and guarantee their unwavering quality and accessibility. The Internet of Things (IoT), which includes machines, sensors, and cameras, continues to steadily expand the number of devices connected to the Internet [96]. Another gauge from the International Data Corporation (IDC) measures that there will be 41.6 billion associated IoT devices, creating 79.4 zettabytes (ZB) of data in 2025 [24].

An intrusion detection system (IDS) is a framework that observe the network traffic and actions and distinguishes any irregular or malicious way of behaving that deviates from the typical or anticipated designs. Intrusion Detection system can be organized into two primary sorts: signature-based technique and anomaly-based technique. Signature-based technique use predefined rules or marks to recognize known attacks, while anomaly-based technique utilize statistical or machine learning strategies to understand the characteristics of legitimate and malicious data during the training/offline phase and identify attacks in incoming traffic during the predicting/online phase. Signature-based technique outputs high accuracy, low false positive rate and faster runtime for known assaults, however, they can't identify novel or unknown assaults, and they require continuous updates of the signature database. Anomaly-based technique relish the value of having the preference to identify new or ambiguous attacks, yet they experience the unfriendly effects of high false-positive rates and high computational intricacy.

Maintaining the security and performance of cyber-physical systems (CPS) on the Internet of Things (IoT) is vital, as these systems often control essential services and infrastructures. The increasing complexity and interconnectivity of these systems have led to a surge in sophisticated cyber-attacks, demanding advanced and flexible intrusion detection methodologies. Current developments in the use of artificial intelligence (AI) have shown promise in enhancing IDS capabilities.

Peer review under responsibility of KeAi Communications Co., Ltd.
[*] Corresponding author.
E-mail addresses: rahmanmahbub073@bit.edu.cn (M.M. Rahman), shahariashakil@bit.edu.cn (S.A. Shakil), mustakim.mizan@bit.edu.cn (M.R. Mustakim).

https://doi.org/10.1016/j.csa.2024.100082
Received 14 May 2024; Received in revised form 19 September 2024; Accepted 17 December 2024
Available online 20 December 2024

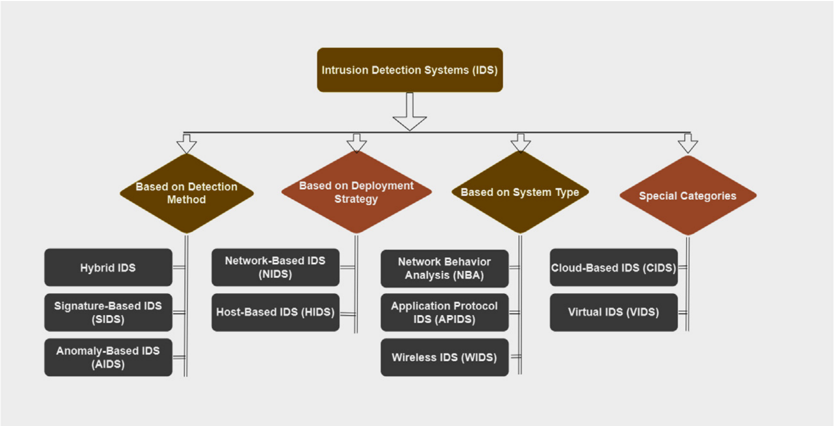

Fig. 1. Overview of Intrusion Detection Systems for IoT Networks.

This advancement enables IoT systems to learn from previous attacks, improving the ability to detect and respond to a wide range of cyber threats. Key challenges in implementing IDS for IoT include dealing with data imbalance, selecting relevant features, managing model complexity, and ensuring adaptability to evolving attack vectors. For instance, Xu et al. (2023) introduced an innovative IDS combining the Binary Grey Wolf Optimizer (BGWO) and Recursive Feature Elimination (RFE) for feature selection, the Synthetic Minority Over-sampling Technique (SMOTE) for data balancing, and XGBoost with Bayesian optimization for classification [96]. This system demonstrated superior results across multiple IoT datasets, achieving high accuracy in both binary and multiclass scenarios. Similarly, Sadhwani et al. [73] proposed a lightweight IDS tailored to the unique challenges of IoT networks, such as handling missing values, data standardization, and feature selection. Their system utilized multiple ML classifiers, including Logistic Regression (LR), Random Forest (RF), Naïve Bayes (NB), Artificial Neural Networks (ANN), and k-Nearest Neighbors (k-NN), achieving near-perfect accuracy on the TON-IOT and BOT-IOT datasets. In another study, Hossain et al. [34] demonstrated the effectiveness of an ensemble-based machine learning approach, which outperformed traditional methods in terms of accuracy and false positive rate. Their method utilized Random Forest as the base classifier and incorporated various feature selection and ensemble strategies, such as correlation analysis, mutual information, principal component analysis (PCA), XGBoost, gradient boosting, bagging, stacking, and AdaBoost. The ongoing exploration of these methodologies highlights the need for continuous innovation in IDS for IoT. For example, Ngo et al. [61] compared different feature selection and extraction methods using the UNSW-NB15 dataset, finding that feature selection methods like Information Gain (IG) and feature correlation significantly improved detection performance and reduced training time. Meanwhile, Tekin et al. [86] investigated on-device ML algorithms for IoT intrusion detection, emphasizing the importance of energy-efficient models that can be deployed on resource-constrained devices. In Fig. 1, addressing these challenges requires continuous innovation and the development of more sophisticated IDS models that can operate efficiently in diverse and resource-constrained IoT environments.

The increasing difficulties in protecting Internet of Things networks are the motivation behind this research. With the rapid adoption of IoT devices across sectors like smart homes, healthcare, and industrial control systems. There is an urgent need for robust intrusion detection systems (IDS) that can effectively detect a variety of cyber-attacks while keeping false positives to a minimum. The diverse applications of IoT, each with its unique data types and attack vectors, require IDS frameworks that are flexible and capable of providing comprehensive protection against a wide range of threats.

Given the constantly changing landscape of IoT security, advancing IDS methodologies remains a crucial area of study. Leveraging machine learning (ML) and deep learning (DL) techniques, along with improved methods for feature selection and data preprocessing, offers a promising path toward developing more effective IDS solutions. This study aims to provide a broad overview of current approaches to intrusion detection in IoT networks, highlight key challenges like data imbalance, model interpretability, and the ability of IDS to adapt to new threats, and suggest directions for future research. Ultimately, the goal is to guide efforts in creating IDS that are better equipped to protect IoT environments against the ever-growing range of cyber threats.

The main contributions of this survey are as follows:

- This survey offers a thorough analysis of the latest intrusion detection techniques and models for IoT networks, evaluating their performance and providing a broad overview of the current landscape. It offers insightful information for developing and putting into practice the upcoming generation of intrusion detection systems. The study also provides an extensive and up-to-date analysis of machine learning-based intrusion detection systems (IDS) for Internet of Things (IoT) networks, covering the concepts and real-world implementations.
- This survey comprehensively reviews data extraction techniques, useful matrices, and loss functions in IDS for IoT networks, ranking the top-cited algorithms. It categorizes IDS studies based on ML/DL models and study focus, including traditional ML models, ensemble-based models, neural networks, deep learning models, and hybrid approaches, summarizing methodologies, datasets, and performance. Additionally, it covers traditional ML models like Support Vector Machines and Naive Bayes, ensemble-based models like Random Forest and AdaBoost, neural networks and DL models like CNNs and LSTMs, etc. Furthermore, the study focus includes survey/literature reviews, lightweight/compact models, feature selection/extraction methods, and specific application areas.
- The study reviews the features, advantages, and disadvantages of several datasets used in IoT intrusion detection. It provides an overview of their characteristics, applications, and significance while comparing the advantages and disadvantages of current IoT security measures across different scenarios. Key findings and conclusions from recent studies are highlighted, detailing categories, benefits, drawbacks, and notable aspects of intrusion detection methodologies. The analysis emphasizes performance metrics and computational efficiency, offering insights into IDS effectiveness and practicality. Standardized evaluation metrics and real-world testing are stressed to ensure reliability. The survey also identifies IoT security challenges, highlighting the need for lightweight, efficient IDS models for resource-constrained devices.
- The study highlights key challenges and unresolved issues in the development of IDS for IoT networks, including constraints like computational complexity and high false positive rates. It also suggests potential research directions, emerging trends, and new perspectives for future work. This forward-looking approach aims to guide and inspire future research efforts in this rapidly evolving field.

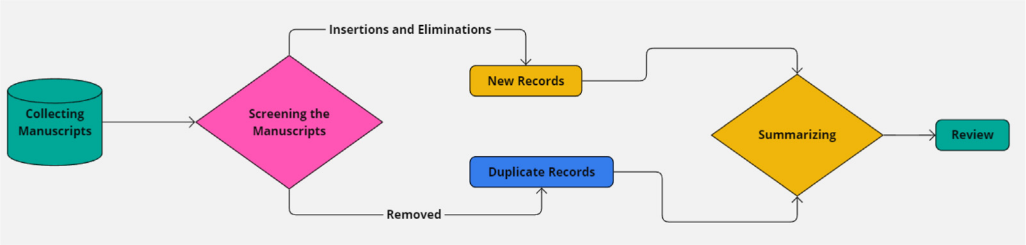

Fig. 2. Summary of articles selection process for IDS in IoT review.

2. Methodology

Methodologies applied to Intrusion Detection Systems (IDS) for Internet of Things (IoT) environments are diverse and constantly evolving, integrating strategies for extracting characteristics from data and using the most recent advancement in different models. This section examines these approaches in detail, focusing on the algorithms and techniques employed for selecting features, preprocessing data, and training models, as well as the datasets commonly used for evaluation purposes.

2.1. Selections of research articles

The process depicted in the provided figure represents a Systematic Literature Review (SLR) methodology, which is widely used in fields such as computer science, software engineering, and information systems. The SLR methodology provides a structured and rigorous approach to reviewing and synthesizing academic literature, ensuring that the review process is comprehensive, transparent, and reproducible shown in Fig. 2.

The review process begins with gathering relevant studies from a wide range of sources, including academic databases, conference papers, and peer-reviewed journals, to ensure a comprehensive collection of existing research. Once these studies are collected, they undergo a screening phase, where they are filtered based on predefined criteria such as relevance, quality, and scope. This step ensures that only the most pertinent and high-quality studies are included. During this phase, any duplicate entries are also identified and removed to maintain accuracy and reduce bias.

Following the initial screening, the process continues with a refinement phase, where newly added records are examined, and any duplicates detected earlier are discarded. This step is crucial for upholding the integrity of the review by confirming that each study is unique and contributes valuable insights. The final stage involves data extraction and synthesis, where the key details from the selected studies-such as research methods, primary findings, and contributions-are compiled to present a summary of the current state of research in the field.

The review phase involves a detailed synthesis and critical analysis of the collected data. During this step, the studies are carefully evaluated to identify patterns, gaps, and key themes within the literature, and conclusions are drawn from the combined findings. This in-depth synthesis helps to clarify the overall state of research in the field, pinpointing important trends, existing challenges, and potential directions for future research. The systematic literature review (SLR) methodology, as shown in the figure, ensures that the review process is both structured and comprehensive, maintaining a high standard of rigor and transparency. By following SLR guidelines, researchers can create reviews that are methodical, replicable, and capable of offering meaningful insights into the specific research question or topic being examined.

2.2. Data extraction techniques

A varied array of data extraction techniques is critical for efficiently detecting and evaluating potential security risks while developing Intrusion Detection Systems (IDS) for Internet of Things (IoT) networks. These techniques include packet capture and analysis, which involves capturing and examining network traffic packets for anomalies using tools like Wireshark or Tcpdump Sheikh et al. [78]; log file analysis, where IoT-generated logs are scrutinized to identify unusual patterns indicative of potential intrusions, often utilizing tools like Splunk and the ELK Stack Sarker et al. [77]; and feature extraction, which focuses on selecting specific data attributes such as traffic volume, packet size, and protocol types that are relevant for detecting intrusions, with machine learning models employing these features to distinguish between normal and malicious activities Gates & Taylor, [28]. In Fig. 3, flow data analysis, utilizing techniques like NetFlow or sFlow, provides insights into communication patterns between devices, helping detect unauthorized or abnormal network activity Moustafa et al. [55].

Data preprocessing and normalization are essential for handling missing values, normalizing data ranges, and encoding categorical variables, ensuring data consistency and improving model accuracy Idowu et al., [36]. Temporal data analysis captures time-series data from IoT devices, which is vital for identifying patterns and anomalies over time Jiang et al., [38]. Contextual data extraction involves capturing information like device types and deployment settings, which aids in understanding the specific characteristics and vulnerabilities of the IoT environment (Sheikh et al., 2020). Metadata extraction, including timestamps and geolocation, provides more insight into the characteristics and context of studied material Sarker et al. [77]. Deep packet inspection (DPI) examines the full content of data packets to detect hidden malware, command and control communications, and data exfiltration activities Moustafa et al. [55]. Statistical feature extraction derives metrics like mean, variance, and entropy from raw data, helping identify deviations from normal patterns that indicate malicious activity Idowu et al. [36]. Application layer data analysis looks for vulnerabilities such as SQL injection and cross-site scripting by analyzing the application-layer protocols (HTTP, DNS, FTP, etc.). Jiang et al. [38]. Behavioral profiling creates profiles for normal behavior of users and devices, with significant deviations potentially indicating intrusions, such as insider threats or compromised devices Sheikh et al. [78]. Encrypted traffic analysis, despite the rise in encryption, can still provide insights into potentially malicious activities by examining traffic patterns and metadata like packet size and timing Gates & Taylor, [28]. Analyzing user and entity behavior to spot anomalous activity, like irregular login patterns or access to private information, is known as User and Entity Behavior Analytics (UEBA). Jiang et al. [38]. By connecting different events to recognize intricate attack patterns, the correlation of multi-source data creates a comprehensive picture for threat detection by combining data from multiple sources, such as network traffic, data logs, and endpoint sensors. Moustafa et al. [55]. Advanced approaches such as deep learning can be used in machine learning-based feature learning to automatically extract features from unprocessed data and identify intricate patterns and relationships that may have gone unnoticed by conventional methods. Idowu et al. [36]. IoT device fingerprinting helps identify and categorize devices based on their network behavior, detecting unauthorized devices on the network Sheikh et al. [78]. Anomaly detection in sensor data is crucial for identifying signs of device malfunctions

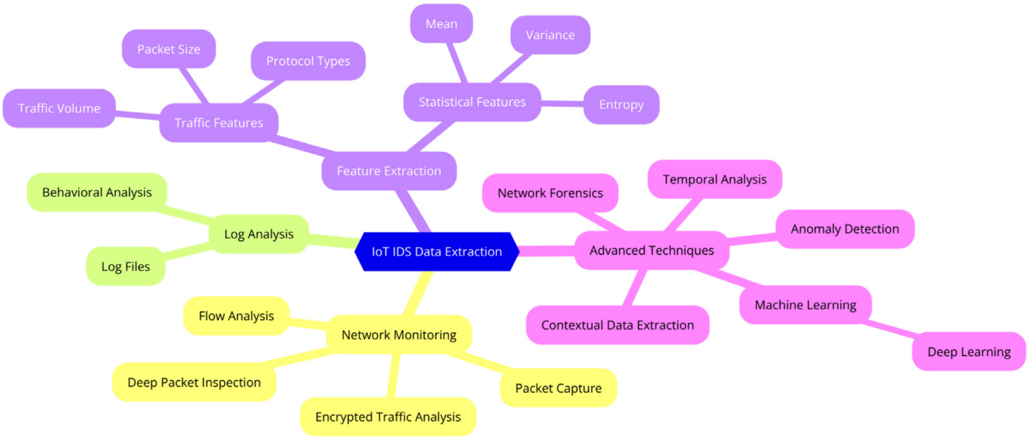

Fig. 3. Overview of Data Extraction Techniques in IDS for IoT Networks.

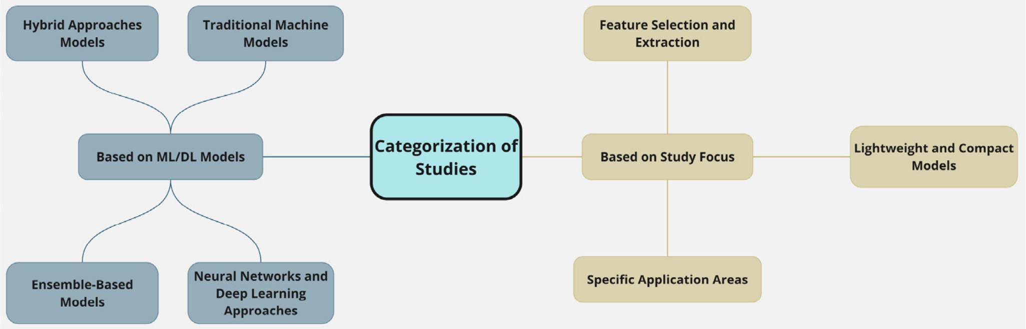
Categorization of Studies
Based on ML/DL Models
Hybrid Approaches Models
Traditional Machine Models
Ensemble-Based Models
Neural Networks and Deep Learning Approaches
Based on Study Focus
Feature Selection and Extraction
Lightweight and Compact Models
Specific Application Areas

Fig. 4. Categorization of Studies on IDS in IoT.

or physical tampering Gates & Taylor, [28]. In network forensics, network traffic is gathered and examined to look into previous security incidents and identify the source and scope of attacks. Moustafa et al. [55]. Finally, threat intelligence integration improves IDS capabilities by delivering real-time information on known threats, such as malicious IP addresses, phishing domains, and malware hashes. Jiang et al. [38], making these comprehensive data extraction techniques essential for robust and reliable security in IoT networks.

3. Studies on intrusion detection systems (IDS) in IoT

The study of IDS (intrusion detection systems) in IoT has seen a variety of methodologies, classified according to the models of machine learning (ML) and deep learning (DL), as well as specialized research focuses. Ensemble-based models like Ada Boost, and Random Forest (RF) have been prominent in ensuring robust network security by integrating multiple algorithms, yielding high accuracy across various datasets such as WSN-DS and UNSW-NB15. Neural networks and DL models, including CNN-BiLSTM and LSTM, offer advanced feature extraction and classification capabilities, often achieving near-perfect accuracy in complex datasets like N-BaIot and BoT-IoT. Traditional ML models, such as automated ML and Naïve Bayes, continue to be relevant, especially in scenarios requiring quick, reliable results with datasets like KDDcup99. As shown in Fig. 4, hybrid approaches blend ML and DL techniques, utilizing methods like SMOTE for data balancing, demonstrating improved detection rates across diverse datasets, including KDDCUP'99 and CIC-MalMem-2022.

The studies were also categorized based on Research focus. Research focus varies from feature selection and extraction to developing lightweight IDS models for real-time application. Specific applications, such as security in IoT Electric Vehicle Charging Stations, highlight the practical implications and challenges in deploying IDS in specialized IoT environments.

3.1. Based on machine learning (ML), or deep learning (DL) models

In this analysis of the most recent exploration during the last several years, we dig into the area that involves machine learning-powered IDS (intrusion detection systems) designed to secure IoT devices. The studies discussed here demonstrate the advanced machine learning approaches to create efficient intrusion detection systems for a variety of IoT scenarios. To improve intrusion detection accuracy, investigators applies a range of methodologies, including ensemble models, deep learning, and feature selection. The collected data from intrusion detection system (IDS) studies summarizes a variety of refined machine learning algorithms and various datasets, representing cutting-edge advances in this domain and reveals a diligent exploration of methodologies to reinforce network security against malicious intrusions. The groundbreaking work of Xu et al. [96] stands out as an example of the effectiveness of ensemble-based methods, which have been the subject of numerous studies. The combination of CNN-BiLSTM, CANET, FNN-Focal, RFS-1, and XGBoost yielded an impeccably balanced IDS, demonstrated by flawless evaluation metrics results. Hossain et al. in keeping with this sentiment, organized an ensemble ballet employing Random Forest, AdaBoost, and gradient boosting algorithms, finishing in a standout accuracy of 99.42% inside the domain of remote sensor networks [34]. Notable, the frequent use of Naïve Bayes as an algorithmic cornerstone, as shown in research like Sadhwani et al. [73] and Vishwakarma et al. [92], showcasing its versatility across unequal backgrounds. Furthermore, the infusion of automated machine learning (AML), as smartly executed by Xu et al. [97], demonstrates the paradigm modification toward automated methodologies, with a standard accuracy of 99.7% achieved in classifying IoT intrusions using the KDDcup99 dataset as

Table 1
Summary of Ensemble-Based Studies.

References	Year	Proposed Methodology	ML/DL Models	Dataset	Performance
Xu et al. [97]	2023	A data-driven method to intrusion and anomaly detection for the IoT based on automated machine learning.	Automated machine learning	KDDcup99	The proposed algorithm cracks a multi-class classification issue with an accuracy of 99.7%, beating the present algorithms.
Ngo et al. [61]	2023	ML-Based Intrusion Detection by Feature Selection and Feature Extraction.	Feature Selection, Feature Extraction, DT, RF, Kneighbors, MLP, Naive Bayes	UNSW-NB15	The statement emphasizes that feature extraction is more reliable than feature selection, especially when the parameter K is small (like 4). It also states that, among of the five classifiers, the decision tree-based MLP is the best for increasing feature selection accuracy in addition as the neural network-based MLP is best for feature extraction.
Viegas et al. [91]	2023	Toward a trustworthy evaluation Schemes for Network-Based Intrusion Detection.	DT, RF, SVM, NB, ANN, and DNN	CIC-IDS2017, CSE-CIC-IDS2018, LUFlow	The DNN model outperforms the other models in terms of accuracy (99%), while the NB model has the lowest false positive rate.
Zakariah et al. [100]	2023	ML-Based Adaptive Synthetic Sampling technique for intrusion detection.	LSTM, CNN	NSL-KDD	The MLP classifier has 87% accuracy in binary classification and performs comparably to the attack and all-class models, with F1 scores of 89% and 83%, and AUC scores of 0.88 and 0.94 respectively.
Gu & Lu [30]	2021	Combining SVM with Naïve Bayes feature embedding to improve data quality and detection performance.	SVM, Naïve Bayes	UNSW-NB15, CICIDS2017	High accuracy, detection rate, low false alarm rate.
Guo et al. [31]	2016	Multiple-criteria time-varying chaos particle swarm optimization Support vector machines and linear programming	SVM, MCLP	NSL-KDD	High rate of detection with a minimal false alarm rate compared to standard PSO and CPSO
Kabir et al. [22]	2018	The optimal allocation-based least square support vector machine (OA-LS-SVM)	LS-SVM	KDD 99	Realistic accuracy and efficiency
Singh et al. [68]	2015	Profiling network traffic and the online sequential extreme learning machine (OS-ELM).	OS-ELM	NSL-KDD 2009, Kyoto University benchmark dataset	Improved accuracy, false-positive rate, and detection time compared to other approaches.

well as Talukder et al. [85] achieved 99.99% on same dataset and 100% on different datasets. Datasets, essential to the logical request, cross-deeply grounded benchmarks like NSL-KDD and UNSW-NB15, close by space-explicit repositories, for example, WUSTL-IIOT-2021 and MQTT-IoT-IDS2020. The continuing emphasis on the evaluation of IDS frameworks on IoT-centric datasets, such as BoT-IoT and ToN-IoT, where the nuanced interaction between LSTM and ANN emerges as a noticeable thematic thread, as Khanday et al. [42] highlight, is notable. The corpus of research extends beyond algorithmic complexities to embrace the pragmatics of real-world deployment, as proved by Rangelov et al. [69], who advocate for the endless enhancement of IoT security measures in urban sceneries. Additionally, Tekin et al. [86] studied the various aspects of on-device machine learning models' energy usage in Smart Home Systems (SHSs). In conclusion, the presented collection of learning demonstrates the vitality of intrusion detection systems by explaining the diverse algorithms and datasets in accordance with the evolving essentials of network security and the rapidly increasing challenges posed by existing threat scenarios. Table 1 presents a list of similar studies and their key results.

1. **Traditional ML Models:** Intrusion detection systems have made significant use of machine learning models because of their ability to recognize and predict hostile activities based on historical data. These models, like Naïve Bayes and Support Vector Machines (SVM), are frequently used due to their ease of use and effectiveness in processing structured data. Traditional ML models are particularly effective in scenarios with well-defined feature spaces and where the relationships between inputs and outputs are relatively straightforward.
2. **Ensemble-Based Models:** Ensemble-based models combine the characteristics of several machine learning methods to increase detection accuracy and durability. By combining predictions from various models, such as Random Forests and AdaBoost, these approaches can reduce the variance and bias associated with single models. Ensemble methods are particularly useful in intrusion detection systems where diverse attack types and patterns need to be detected across different data sources.
3. **Deep Learning and Neural Networks Models:** In the past few years, neural networks and deep learning models have gained prominence due to their ability to detect complex patterns and representations in large datasets. Models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are particularly effective at processing high-dimensional data and understanding temporal sequences. Deep learning approaches excel at recognizing subtle anomalies and patterns that may be missed by traditional methods.
4. **Hybrid Approaches:** Hybrid approaches in intrusion detection combine multiple methodologies, including deep learning, traditional machine learning, and other techniques to enhance detection capabilities. These approaches often integrate feature classification, selection, and extraction techniques. By combining the capabilities of several models and methodologies, hybrid systems can offer more complete and robust solutions to difficult security concerns.

3.2. Based on study focus

1. **Specific Application Areas:** The table presents a summary of research studies in specialized fields. These studies address various difficulties and offer solutions designed for particular settings, including cyber-physical systems (CPS), software-defined networks (SDNs), industrial control systems (ICS), and in-vehicle networks. The research underscores progress in anomaly detection, intrusion detection systems, and the adoption of innovative machine learning models to improve security and efficiency in these specific sectors.
2. **Feature Selection/Extraction:** This table summarizes works that focus on feature selection and extraction strategies. These studies investigate diverse methodologies, including Naïve Bayes feature embedding, genetic algorithms, and hybrid approaches integrating ML and DL models. The findings emphasize the importance of refining

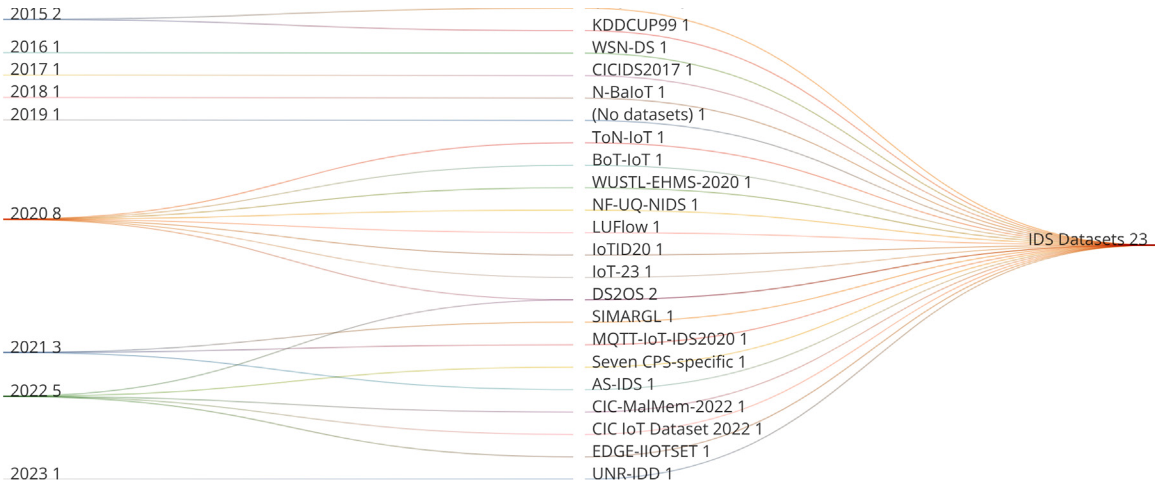

Fig. 5. Dataset Distribution Over Years for IDS in IoT Networks.

feature selection and extraction processes to improve the accuracy, efficiency, and reliability of security frameworks.

3. **Lightweight/Compact Models:** The table highlights research focused on developing lightweight and compact intrusion detection systems (IDS) that maintain high performance while being resource-efficient. The studies investigate various ML based classifiers, DL models, and optimization strategies to create IDS solutions that are suitable for environments with limited computational resources. The emphasis is on achieving high accuracy and reducing false alarm rates without compromising on speed and efficiency.
4. **Survey/Literature Review:** This table presents comprehensive surveys and literature reviews that analyze existing intrusion detection techniques, datasets, and challenges. These reviews provide insights into the effectiveness of various methods, highlight key trends, and identify potential areas for future research. The emphasis is on providing a comprehensive overview of the current status of IDS research, including the application of machine learning techniques and the changing environment of cybersecurity threats.

4. Dataset and evaluation metrics

4.1. Dataset

In today's dynamic cybersecurity world, evaluating and developing intrusion detection systems (IDS) is significantly reliant on broad and representative information. These datasets are critical benchmarks for developing and testing artificial intelligence for detecting and responding to various cyber threats. A summary of the experiments conducted by numerous researchers on the detection of DDoS attack on IoT-based networks using ML is shown in Tables 1 and 2. The majority of this research focused on a DDoS attack on older datasets such as NSL-KDD, WSN-DS, UNSW-NB15, KDDCUP/KDDcup99, IoT-23, CICIDS / CIC-IDS2017/CSE-CIC IDS2018, Seven CPS-specific, and DS2OS.

Fig. 5 shows the release of IDS (intrusion detection system) datasets for the Internet of Things (IoT) from 2015 to 2023. It indicates that datasets like UNSW-NB15 and KDDCUP99 were released in 2015, followed by WSN-DS in 2016 and CICIDS2017 in 2017. N-BaIoT was introduced in 2018, while 2019 had no significant new datasets. The year 2020 saw a surge with datasets like ToN-IoT, BoT-IoT, and IoTID20. In 2021, datasets such as SIMARGL and AS-IDS were added, and 2022 featured releases like Seven CPS-specific and CIC-MalMem-2022. The most recent dataset, UNR-IDD, was introduced in 2023. This diagram provides a visual representation of the flow and accumulation of these datasets over time, showing their contribution to the field of IDS for IoT networks.

Intrusion Detection Systems (IDS) designed for IoT networks have primarily relied on datasets published in the past. Our research, however, aims to evaluate the current landscape of Distributed Denial of Service (DDoS) attack intensities, the complexities associated with IoT devices, and the limitations of the datasets currently available. With evolving attack strategies, it's clear that there is a pressing need to update these datasets to reflect more recent threats. Table 3 provides a detailed overview of the shortcomings and constraints of the datasets presently used in IoT network research.

It is worth noting that some widely referenced benchmark datasets, such as CIC-IDS2017, UNSW-NB15, and NSL-KDD, were not originally created in an IoT-specific environment. Moreover, several datasets, including TON_IoT and Bot-IoT, suffer from class imbalances, which can introduce biases or inaccuracies, complicating the process of accurately identifying attacks. Additionally, datasets like UNSW-NB15 and NSL-KDD (associated with the KDD Cup 1999) that have been utilized for DDoS detection do not fully cover all types of DDoS attacks. Meanwhile, datasets like N-BaIoT2018 and Bot-IoT focus on only a few DDoS attack types, such as TCP, UDP, and HTTP.

The following table provides an overview of key datasets employed in network security and intrusion detection research. These datasets vary in their release and update dates, providers, advantages, and potential limitations, offering diverse resources for cybersecurity applications. They span a range of contexts, from general IoT environments to specific industrial settings, equipping researchers and practitioners with the tools needed to enhance intrusion detection techniques. Understanding both the strengths and weaknesses of these datasets is crucial for developing effective and adaptable IDS solutions. Let's explore the key characteristics of these datasets in detail.

4.2. Evaluation matrices

In various fields, particularly in evaluating performance, security, and quality, several key metrics are used to assess the effectiveness of systems and models. Accuracy measures the correctness of predictions by calculating the ratio of correct predictions to the total number of cases. Precision focuses on the accuracy of positive predictions, indicating the model's ability to minimize false positives. Recall, or sensitivity, measures the model's ability to identify all relevant instances, reflecting the rate of false negatives. The F1-Score, a harmonic mean of precision and recall, offers a balanced measure when considering both false positives and false negatives. The False Positive Rate (FPR) assesses the proportion of incorrect positive predictions among actual negatives, which is critical in contexts like medical testing or fraud detection. Detection Rate and True Positive Rate (TPR) both highlight the model's efficacy in

Table 2
Summary of Ensemble-Based Studies.

References	Year	Proposed Methodology	ML/DL Models	Dataset	Performance
Hossain et al. [34]	2023	Using ensemble-based machine learning to provide network security.	RF, AdaBoost, gradient boosting.	UNSW-NB, UNR-IDD, UKM-IDS, SIMARGL, NSL-KDD, KDDCUP, CICIDS, and WSN-DS, etc.	Highest accuracy of 99.42% for WSN-DS, 97.77% for UNSW-NB15
Sadhwani et al. [73]	2023	Compact and lightweight IDS that blends ML classifiers	RF, NB, LR, ANN, KNN	BoT-IoT and ToN-IoT	RF did great with TON-IOT, and NB performed well with BOT-IOT, scoring 100% accuracy in both binary and multiple-class classification. They also trained and predicted faster.
Musleh et al. [57]	2023	Machine learning algorithms used with feature extraction in an IoT-based intrusion detection system.	A number of feature extractors, such as DenseNet and VGG-16 transfer learning models and image filters	IEEE Dataport	The findings revealed that the integration of VGG-16 with stacking led to the greatest accuracy, achieving a remarkable 98.3%.
Kumar et al. [43]	2023	Used statistical feature ranking methods and machine learning for intrusion detection	Naive Bayes	N/A	Upon assessing accuracy values, the authors determine that removing the two features with the lowest values enhance accuracy, resulting in a peak accuracy of 95.69% using the top 7 features instead of utilizing all 9 features.
Krishnan et al. [65]	2019	Developing VARMAN, a multi-plane security framework integrating hybrid machine learning models.	Non-Symmetric Deep Autoencoder, Random Forest	NSL-KDD, CICIDS2017, HogZilla	High accuracy, effective anomaly detection, efficient resource utilization.
Hamed et al. [83]	2018	Recursive feature addition and bigram technique	Recursive Feature Addition (RFA) with SVMs	ISCX 2012	Notable improvement in performance using different metrics
Singh et al. [39]	2023	Feature reduction using Random Forest Classifier, SelectFromModel, Recursive Feature Elimination (RFE), and evaluation using multiple machine learning classifiers.	Random Forest, Extra Trees, AdaBoost, SVM	NSL-KDD	Various metrics (accuracy, F-score, precision, recall) across different attack categories (DoS, Probe, R2L, U2R)
J.A. & K.A. [37]	2023	Implementing FL with various ML models, synchronization methods, and aggregation techniques.	LSTM, CNN, Random Forest, MLP	NSL-KDD, VeReMi, CAN-Intrusion, Car Hacking dataset	Evaluation using F1-Score, Accuracy, Precision, Recall
Ravi et al. [9]	2022	Feature fusion ensemble meta-classifier	RNN, LSTM, GRU, SVM, Random Forest, Logistic Regression	KDD-Cup-1999, UNSW-NB15, WSN-DS, CICIDS-2017	WSN-DS: 0.98 accuracy, KDD-Cup-1999: 0.99 accuracy, UNSW-NB15: 0.99 accuracy, and CICIDS-2017: 0.99 accuracy
Alazzam et al. [32]	2021	Fusion of two subsystems trained on normal and attack packets using OCSVM and PIO.	OCSVM	KDDCUP-99, NSL KDD, UNSW-NB15	99.9% DR, 0.06 FPR, 99.3% accuracy

identifying all relevant cases, which is crucial in security and threat detection systems. Lastly, Detection Accuracy combines the assessment of both positive and negative case identifications, providing a comprehensive measure of a system's overall performance. These metrics are essential for optimizing operations and enhancing decision-making across various domains.

The following table summarizes the most useful matrices commonly used for evaluating Intrusion Detection Systems (IDS) in IoT networks.

5. Comprehensive analysis of key findings

5.1. Analysis of machine learning models in IoT IDS

Intrusion Detection Systems on IoT deploy a varied array of methods to boost security and detect malicious activities. In our research, we investigated the common use and applicability of several ML methods across various types of studies. The data, illustrated in a comprehensive pie chart, underscores the widespread use of algorithms like Random Forest (RF), Gradient Boosting, Naive Bayes (NB), AdaBoost, and Logistic Regression (LR), which are often chosen for their reliability and precision in classification tasks. Additionally, Artificial Neural Networks (ANN), including specialized forms such as CNN and DNN, provide effective solutions for managing complex data patterns. Additionally, algorithms like K-Nearest Neighbors (KNN), Decision Tree (DT), and Support Vector Machines (SVM), along with advanced ensemble methods such as XGBoost and Stacking, contribute to effective feature selection and classification. Specialized approaches, including Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and hybrid methods like Hybrid GA-GWO (Genetic Algorithm + Grey Wolf Optimizer), are also explored for optimizing model performance. The integration of techniques such as SMOTE for Data Balancing, Feature Selection, and innovative models like MLEID (Machine Learning-based Ensemble Intrusion Detection) and SDRK Machine Learning Algorithm (Supervised Deep Neural Networks + Unsupervised Clustering), reflects the evolving landscape of IDS in IoT, emphasizing the need for adaptive and sophisticated methods to secure IoT ecosystems as shown in Fig. 6.

This analysis not only highlights the versatility and performance considerations of these algorithms but also sheds light on the evolving landscape of machine learning methodologies. The presence of cutting-edge techniques, including Variational Autoencoders (VAEs) and Deep Convolutional Generative Adversarial Networks (DC-GAN), further indicates a shift towards more complex and sophisticated models, paving the way for future research endeavors. Additionally, the chart showcases a variety of less common algorithms, demonstrating the diverse methodologies utilized in the field. This analysis offers meaningful insights into the prevailing trends and the relative popularity of various machine

Table 3
A Summary of research on Deep Learning models and Neural Networks.

Ref.	Year	Proposed Methodology	ML/DL Models	Dataset	Performance
Xu et al. [96]	2023	ML-based approach to developing an IDS for IoT devices.	CNN-BiLSTM, CANET, FNN-Focal, RFS-1, XGBoost, XGBoost-HPO, XGBoost-HPO-feature-selection	BoT-Iot, NSL-KDD, WUSTL-IIOT2021, N-BaIot, and WUSTL-EHMS-2020.	The model attained perfect scores in accuracy, precision, recall, and an F1 score of 1.0, which strongly indicates its effectiveness.
Khanday et al. [42]	2023	A lightweight IDS with a novel data pre-processing technique while using ML and DL classifiers.	Linear SVC, Naïve Bayes, Logistic Regression, ANN, LSTM	BoT-IoT and ToN-IoT	The LSTM and ANN models performed the best in both datasets for binary and multiple classifications, with 99% and 95% accuracy, respectively.
Gaber et al. [27]	2023	PSO and Bat algorithm for picking vital features and employs the RF classifier to identify malicious activities in IIoT network traffic.	RF classifier along with Bat algorithm (BA), KNN, MLP	WUSTL-IIOT-2021	RF on a dataset created from the BA scheme scored the highest value of 99.99%.
Vishwakarma et al. [92]	2023	A novel two-phase Intrusion Detection System (IDS) utilizing Naïve Bayes for data classification and an elliptic envelope approach for anomaly detection has been proposed.	NB, elliptic envelop method	NSL-KDD, UNSW_NB15, and CIC-IDS2017	The suggested method obtained reasonable accuracy in the first phase, with 97.5% accuracy in the NSL-KDD dataset, 86.9% in the UNSW_NB15 dataset, and 98.59% in the CIC-IDS2017 dataset.
Rangelov et al. [69]	2023	Towards an integrated methodology and tool chain for urban IoT networks and platforms.	MLP, DNN, CNN, and LSTM	N/A	The authors aim to deploy and continuously improve suitable IoT security measures in real-world urban IoT frames.
Thakur et al. [71]	2021	Combining generic and domain-specific autoencoders to extract and classify network intrusions.	Generic-Specific Autoencoder, Random Forest	CICIDS2017	High precision, recall, specificity, F1 scores.
Wu et al. [99]	2020	Semantic re-encoding and Deep Learning	Deep Learning (ResNet)	NSL-KDD	On the NSL-KDD dataset, the SRDLM algorithm outperforms traditional machine learning approaches by more than 8% and detects Web character injection network attacks with over 99% accuracy.
Seo et al. [25]	2023	GAN-based method to generate adversarial attacks.	Multi-layer perceptron (MLP), random forests (RF), logistic regression (LR)	Fuzzy attack dataset of Hyundai YF Sonata	Hyundai YF Sonata: Training: 403,299 samples (318,655 normal, 84,644 attack), Testing: 351,273 samples (276,337 normal, 74,936 attack)
Akkepalli & Sagar [82]	2024	Hybrid model combining CNN for spatial features; Bi-LSTM for temporal features.	CNN, Bi-LSTM	NSL-KDD dataset	The model achieved accuracy: 99.28%, precision: 99%, recall: 99.26%, and F1-Score: 99.18%.
Doriguzzi-Corin & Siracusa [21]	2024	Enhancing DDoS attack detection using adaptive federated learning.	Adaptive Federated Learning (FLAD)	CIC-DDoS2019	FLAD outperforms other models (FedAVG, FLDDoS) in terms of F1 score and time
Thein et al. [84]	2024	Improving intrusion detection in IoT using personalized federated learning and robust defense mechanisms.	Personalized Federated Learning-based IDS (pFL-IDS)	N-BaIoT dataset	CNN
Maddu & Rao [53]	2023	CenterNet-based feature extraction, ResNet152v2-based classification, and DCGAN for data augmentation.	CenterNet, ResNet152v2, DCGAN	InSDN dataset, Edge IIoT dataset	InSDN dataset: 99.65% accuracy, Edge IIoT dataset: 99.31% accuracy
Fang et al. [98]	2024	Use of genetic algorithms for feature selection in intrusion detection systems	Not specified explicitly	Various datasets used in the industrial control systems for testing	Enhanced performance metrics.

learning methods, highlighting both commonly used techniques and less-explored areas that may present opportunities for future research.

The bar chart illustrates the top 10 algorithms used in IoT intrusion detection, ranked by the number of citations they have received in research articles. Random Forest (RF) stands out as the most cited algorithm with 12 citations, showcasing its widespread application and effectiveness in this domain. SVM is the second-largest algorithm used in various papers cited over 7 articles. MLP, LSTM and CNN are also highly cited, each with 5 citations, indicating their strong presence in the literature. K-Nearest Neighbor (KNN) and Gradient Boosting follow with 6 citations each, highlighting their significant roles in IoT security. The Artificial Neural Network (ANN) is cited 5 times, reflecting its specialized use. XGBoost, Decision Tree (DT), and Logistic Regression (LR) each have 4 citations, demonstrating their relevance. J48, with 2 citations, is less frequently mentioned but still notable. This ranking showcase the insights on the most impactful algorithms in the realm of IoT intrusion detection.

5.2. *Analysis of key findings in IoT IDS*

The understandings highlight different algorithms and methods custom-made to handle explicit difficulties in getting IoT networks.From lightweight models with imaginative data pre-processing to hybrid techniques consolidating ML and DL, these discoveries offer significant experiences for network protection experts and specialists exploring the intricacies of IoT security. Fig. 7 depicted the field of intrusion detection in IoT network environments is rapidly evolving, necessitating complicated approaches to dealing with and defending against emerging threats.

Table 12 gives brief outlines of key discoveries and decisions from different arrangements of ongoing inspections in this space. Each entry captures the strengths, limitations, and notable aspects of the respective intrusion detection methodologies. From novel coordination ways to deal with algorithmic subtleties and dataset contemplations, these bits of knowledge add to a thorough comprehension of the present sta-

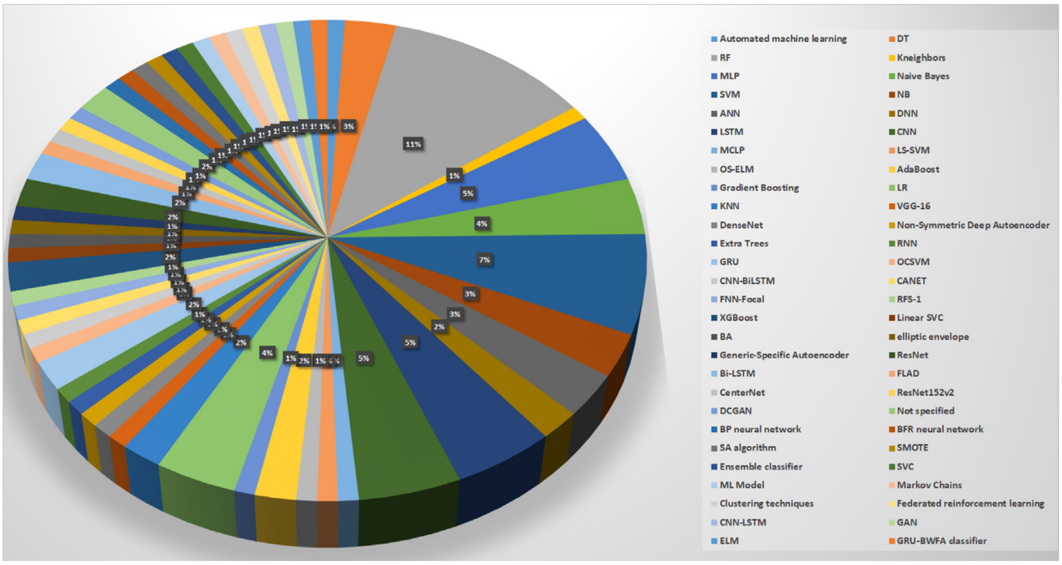

Fig. 6. Distribution of Articles Across Machine Learning Algorithms.

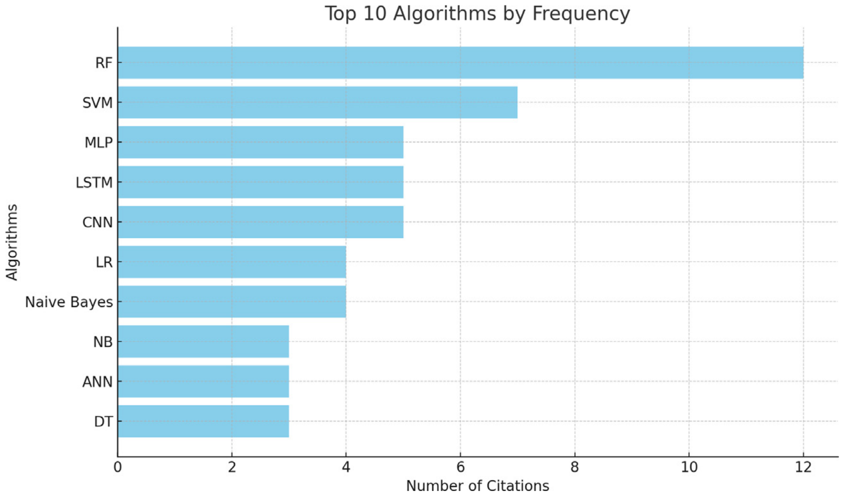

Fig. 7. Top 10 IoT Intrusion Detection Algorithms by Citations.

tus and difficulties in IoT security. As we dive into the complexities of each review, it becomes apparent that while progressions are promising, cautious thought of constraints and future exploration needs is essential to refining and propelling the viability of interruption identification frameworks in the powerful domain of IoT.

5.3. Analysis of loss functions in IDS for IoT networks

In Intrusion Detection Systems (IDS) for IoT Networks, various loss functions play a crucial role in optimizing model performance. These functions guide the training of machine learning and deep learning models by minimizing the difference between predicted and actual values, thus enhancing the accuracy of intrusion detection. For classification tasks, Cross-Entropy Loss is widely used, measuring the performance of models that output probability values, which is essential for distinguishing between normal and malicious traffic [20]. Meanwhile, regression tasks typically use Mean Squared Error (MSE) and Mean Absolute Error (MAE), both of which focus on the differences between predictions and actual outcomes, proving useful in anomaly detection models [13,46].

In more specialized classification approaches like Support Vector Machines (SVMs), Hinge Loss penalizes incorrect classifications, maximizing the margin between classes and improving the model's robustness to network attacks [16]. Kullback-Leibler Divergence (KLD) further enhances performance by quantifying the difference between two probability distributions, making it effective in measuring anomalies in IoT networks [102]. In Fig. 8 demonstrated, the Brier Score Loss helps in evaluating the confidence of binary classification models, making it particularly useful for detecting intrusions in binary settings [62].

A critical challenge in IDS for IoT is dealing with imbalanced datasets, where rare but crucial intrusion events can be overshadowed by more frequent, benign data. Loss functions like Focal Loss and Tversky Loss address this by emphasizing the detection of these rare events, improving the detection rate for critical intrusions [4,80]. Additionally, robust loss functions like Huber Loss and MAE help models maintain performance even in the presence of noisy or anomalous data, ensuring the stability of predictions [41].

In complex scenarios involving multi-label and multi-class problems, Jaccard Loss, Hamming Loss, and Sparse Categorical Cross-Entropy Loss come into play. These loss functions are designed to handle overlapping categories and sparse data, improving the performance of models tasked with identifying multiple, simultaneous intrusion types [51,67,87]. Finally, for models focusing on specific performance metrics, AUC Loss and Kappa Loss are used to optimize the area under the ROC curve and Cohen's Kappa statistic, respectively, ensuring that the models not

Table 4
Summary of hybrid Models Studies.

References	Year	Proposed Methodology	ML/DL Models	Dataset	Performance
Wadate et al. [93]	2023	Edge-Based Intrusion Detection using ML Over the IoT Network.	Backpropagation (BP) neural network, Basis function Radial (BFR) neural network, Simulated Annealing algorithm.	KDD99	The proposed IDS demonstrate the highest accuracy, reaching up to 93%. In contrast, the accuracy of the Naive Bayes detection is the lowest, which could be attributed to its use of a BP neural network.
Talukder et al. [85]	2023	A novel hybrid approach that blends ML and DL to boost detection rates while maintaining reliability.	SMOTE for data balancing, XGBoost for feature selection	KDDCUP'99 and CIC-MalMem-2022	The accuracy achieved from testing on two different datasets was remarkably high, reaching 99.99% and a perfect 100% respectively.
Vanitha et al. [90]	2023	Improved AnT colony optimization and machine learning-based ensemble Intrusion Detection model	DT, SVM, Ensemble classifier, Proposed MLEID	UNSW-NB15	The new MLEID classifier's overall findings are 98.34%, whereas smaller rates of precision for classifiers like DT, SVM, and Ensemble are 77.67%, 89.67%, and 94.34%, respectively.
Ahuja et al. [58]	2021	Hybrid model combining SVC and Random Forest	SVC, Random Forest	Custom SDN Dataset	Accuracy: 98.8%, and very low false alarm rate.
Fazio et al. [64]	2020	Using Markov chains to model probabilistic packet marking for IP traceback.	Markov Chains	Simulated Network Data	High traceback accuracy, minimal overhead.
Gupta et al. [1]	2018	Training-resistant anomaly detection system	Anomaly detection using clustering techniques	Various real network traffic data sources	Resistant to training attacks, effective against common network attacks
Vadigi et al. [72]	2023	Enhancing IoT security using federated reinforcement learning.	Federated reinforcement learning (FRL) for IDS	IoT datasets	Reinforcement learning models
Li et al. [7]	2024	An intrusion detection system for hybrid DoS attacks (HDA-IDS), CL-GAN	CNN-LSTM, GAN	NSL-KDD, CICIDS2018, Bot-IoT	In comparison to other works, the HDA-IDS achieved an average overall improvement of 5% in terms of accuracy, precision, recall, and F1-Score.
Melucci [54]	2024	Spectral decomposition of mixtures of symmetric matrices	Not specified	Large test collection for IR	The method effectively balances ranking effectiveness with fairness.
Hoang & Kim [33]	2024	Supervised contrastive learning, ResNet, transfer learning	Supervised contrastive ResNet	Car Hacking dataset, survival dataset	Compared to the vanilla cross-entropy loss, the SupCon loss averagely reduces false-negative rates by five times.
Sanju [74]	2023	It used Modified Metaheuristics with Weighted Majority Voting Ensemble Deep Learning (MM-WMVEDL)	BiLSTM, ELM, GRU	IoT-23, UNSW-NB15, CICIDS2017	IoT-23: 98.12% accuracy, CICIDS2017: 99.98% accuracy, UNSW-NB15: 97.34% accuracy
Rajasekaran & Magudeeswaran [66]	2023	GRU-BWFA classifier with Enhanced Salp Swarm Optimization for feature selection	GRU-BWFA classifier	UNSW-NB15, NSL-KDD	UNSW-NB15, NSL-KDD datasets

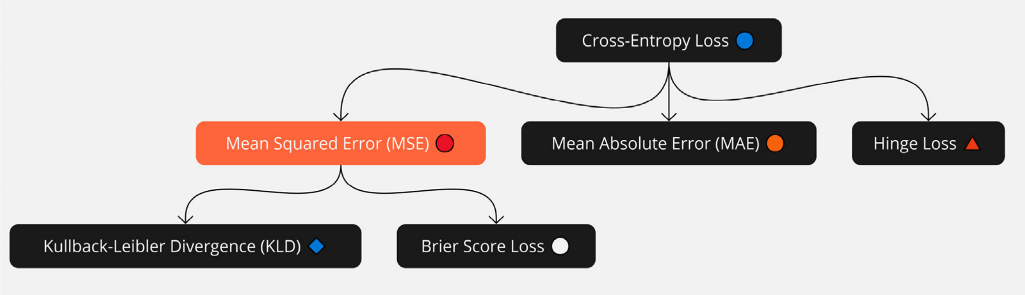
Cross-Entropy Loss ●
Mean Squared Error (MSE) ●
Mean Absolute Error (MAE) ●
Hinge Loss ▲
Kullback-Leibler Divergence (KLD) ◆
Brier Score Loss ●

Fig. 8. Most Useful Loss Functions.

only classify intrusions accurately but also provide reliable confidence in their predictions [49,95].

Thus, the choice of loss function in IDS for IoT Networks is pivotal in ensuring that the models can robustly and accurately detect intrusions, even in challenging environments with noisy data and imbalanced datasets. Each loss function plays a specialized role, contributing to the overall efficacy and reliability of the intrusion detection system.

5.4. Analysis of performance metrics and computational efficiency

IDS plays an essential role in detecting and responding to malicious activities in the network environment. Evaluating the performance and computational efficiency of IDS models is critical to assuring their effectiveness and stability. The following table summarizes key performance metrics and their importance in assessing IDS models.

6. Challenges, open issues and gap analysis

According to the data presented in Tables 1–11,13 this analysis aims to identify the main challenges, unresolved issues, and gaps in the current research landscape in the rapidly developing field of intrusion detection systems (IDS) for Internet of Things (IoT) environments. Researchers have developed various methodologies using a wide range of ML and DL models supported by numerous datasets. These combined studies and datasets offer critical insights into the strengths and limitations of current intrusion detection methods.

6.1. Most prominent challenges

A key challenge highlighted in the studies is the diversity of IoT datasets used. Popular datasets like UNSW-NB15 and NSL-KDD are fre-

Table 5
Summary of Specific Application Areas Studies.

References	Purpose	Main Findings	Trend and Focus
Krishnan et al. [65]	Develop a multi-plane security framework for SDN	The combination of hybrid ML techniques and NDAE significantly improves IDS performance and resource optimization in SDNs.	Integrating advanced machine learning techniques with SDN to develop scalable and efficient security frameworks.
Thakur et al. [71]	Enhance IDS in CPS with deep autoencoder models	The unique architecture of GSAE effectively disentangles generic and domain-specific features, leading to improved classification performance.	Developing deep learning models that can handle the complexities and variations of network intrusions in CPS.
Ahuja et al. [58]	Classify benign and DDoS attack traffic in SDN environments	The proposed hybrid ML model significantly improves DDoS attack detection accuracy and reduces false alarms compared to existing methods.	Enhancing DDoS attack detection in SDN environments using advanced ML techniques and custom datasets for better accuracy and reliability.
Satheesh et al. [59]	Develop a priority-based model using SDN to detect anomaly intrusions	Flow-based ML models combined with SDN provide a robust framework for real-time anomaly detection and network management, outperforming conventional methods.	Leveraging SDN's capabilities for centralized control and dynamic response to enhance network security through advanced ML techniques.
Fazio et al. [64]	Model probabilistic packet marking for IP traceback	Modeling the PM approach using Markov chains provides a systematic and efficient method for IP traceback, reducing the number of packets required for accurate path reconstruction.	Emphasizes the use of probabilistic and stochastic models to enhance network security mechanisms, particularly for mitigating DoS and DDoS attacks.
Kabir et al. [22]	Develop a comprehensive multi-plane security framework for SDN	OA-LS-SVM effectively detects intrusions with a realistic performance.	Improving intrusion detection through statistical techniques and optimization.
Gupta et al. [1]	Enhance IDS in CPS by combining generic and domain-specific deep autoencoders	Training attacks can be detected and the IDS remains effective.	Enhancing IDS resilience against training-based attacks.
Singh et al. [68]	Develop a priority-based model using SDN to detect anomaly intrusions	OS-ELM with traffic profiling is efficient and effective for NIDS.	Reducing complexity and improving performance in IDS using OS-ELM.
Wu et al. [99]	Model probabilistic packet marking for IP traceback	Semantic re-encoding and deep learning significantly improve the accuracy and robustness of the intrusion detection model.	Enhancing generalization ability and robustness of IDS using semantic re-encoding combined with deep learning.
Truong et al. [8]	Detect cyberattacks in ICS using anomaly detection	The proposed method effectively detects cyberattacks in industrial control systems.	Anomaly detection is a viable approach for securing industrial control systems.
Vadigi et al. [72]	Propose a federated reinforcement learning-based IDS for enhancing IoT security	The proposed system effectively detects intrusions in IoT environments using FRL.	FRL enhances the security of IoT systems by improving detection accuracy.
Doriguzzi-Corin & Siracusa [21]	Propose an adaptive federated learning approach for detecting DDoS attacks	The proposed approach effectively detects DDoS attacks with high accuracy.	Adaptive federated learning improves the detection of DDoS attacks.
Boobalan et al. [63]	Explore the integration of federated learning with IIoT	The integration of FL with IIoT provides significant security and efficiency improvements.	Federated learning enhances the security and operational efficiency of IIoT systems.
Thein et al. [84]	personalized federated learning method	proposed pFL-IDS effectively detects intrusions and mitigates the impact of poisoning attacks.	Personalized federated learning enhances IDS performance and robustness against poisoning attacks.
Li et al. [7]	Address security challenges in IoT networks with hybrid IDS	In terms of botnet and DoS attack detection, the HDA-IDS performs better than other IDS.	Improving IoT security using hybrid detection methods and advanced AI models.
Melucci [54]	Maximize ranking effectiveness and fairness in information retrieval systems	Maintaining an acceptable level of effectiveness and fairness simultaneously is feasible.	Balancing effectiveness and fairness in information retrieval systems.
Hoang & Kim [33]	Propose a deep learning model for in-vehicle IDS	The SupCon ResNet model effectively classifies multiple attacks and adapts to new vehicle models.	Enhanced performance by using contrastive learning and transfer learning.
Khan et al. [40]	Develop method for detecting intrusion attacks on in-vehicle CAN	Effective detection of in-vehicle network intrusions using the proposed method.	Security in automotive networks.
Zhu et al. [103]	Enhance transferability of adversarial attacks using hybrid approach	Hybrid attacks can significantly improve adversarial transferability.	Enhancing the effectiveness of adversarial attacks.
Rehman et al. [70]	Enhance IoT security using proactive defense mechanisms	Proactive defense mechanisms can significantly enhance IoT security.	Focus on proactive security measures in IoT.
Abolfathi et al. [3]	Enhance web privacy on HTTPS traffic with novel method	The novel method significantly enhances web privacy.	Enhancing privacy on web traffic.
Sanju, [74]	Propose hybrid approach for IDS in IoT	The proposed hybrid technique increases the accuracy and efficiency of IDS in IoT systems.	Focus on addressing the physical and functional variety of IoT systems.
Gupta et al. [79]	Develop efficient IDS for IoT-enabled smart cities using hybrid optimization and deep learning	The hybrid approach significantly enhances classification accuracy and reduces training time.	Focus on improving IDS performance in IoT-enabled smart cities.
Shone et al. [60]	Develop IDS using transformer-based models for improved detection of network intrusions	Transformer-based models improve the detection capabilities of IDS in network environments.	Focuses on advanced transformer models.
Rajasekaran & Magudeeswaran, [66]	Detect malicious attacks in network environments using GRU-BWFA classifier	Proposed classifier effectively detects and differentiates various types of network attacks with high accuracy.	Improve the detection of cyber-attacks using advanced classification techniques.
Seo et al. [25]	Introduce GAN-based adversarial attacks in in-vehicle networks	GAN-based adversarial attacks can significantly reduce the detection accuracy of ML-based IDS in in-vehicle networks.	Focus on improving the adaptability of ML-based IDS to adversarial attacks.
Akkepalli & Sagar, [82]	Propose hybrid CNN, Bi-LSTM model for effective network anomaly detection	In network anomaly detection, the hybrid CNN and Bi-LSTM model performs better than other models.	Improvement using hybrid DL models.
J.A., K.A. [37]	Explore FL for IDS in IoV	Highlighted the effectiveness of FL in IoV contexts for improving IDS performance while maintaining data privacy.	Increasing interest in FL to enhance security in IoV by decentralizing the learning process.
Al-Ghuwairi et al. [10]	Detect anomalies in cloud computing using time series data and ML	Demonstration on applicability of time series models for improving IDS in cloud environments.	Focus on real-time anomaly detection and continuous monitoring in cloud computing.
Maddu & Rao, [53]	Implement CenterNet-ResNet152V2 based deep learning technique for SDN	The suggested model has great detection capabilities and can effectively mitigate and identify the source of attacks.	Future work will involve strengthening the system through feature selection, detecting zero-day and lowering the rate of DDoS attacks on IoT systems.
Rangelov et al. [69]	Integrated methodology for ML-based IDS in urban IoT networks.	IoT security mechanisms are being continuously improved in urban IoT.	Enhancing IoT security in urban networks.
ElKa-shlan et al. [23]	ML-based intrusion detection system for IoT electric vehicle charging stations (EVCSs).	Classified attacks with 99.2% accuracy using filtered classifier algorithm.	Enhancing security of IoT EVCSs using ML-based IDS.

Table 6
Summary of Feature Selection/Extraction Studies.

References	Purpose	Main Findings	Trend and Focus
Gu & Lu, [30]	Improve IDS by merging Naïve Bayes feature and SVM.	When SVM and Naïve Bayes feature embedding are used, IDS performance is greatly enhanced. The method is effective and adaptable to different datasets and environments.	Enhancing ML models for intrusion detection by improving data quality and integrating hybrid techniques to boost performance.
Guo et al. [31]	Improve IDS by merging Naïve Bayes feature and SVM	TVCPSO improves SVM and MCLP by optimizing parameter setting and feature selection.	Optimizing traditional ML models with advanced optimization techniques.
Hamed et al. [83]	Classify benign and DDoS attack traffic in SDN environments	RFA and bigram technique improve NIDS performance significantly.	Combining feature selection methods with ML for better NIDS.
Ravi et al. [9]	Propose feature fusion ensemble meta-classifier for IDS	Feature fusion and ensemble meta-classifier enhance the detection and classification of network intrusions.	Improved network intrusion detection can be achieved by incorporating feature fusion with ensemble learning.
Singh et al. [39]	Develop efficient IDS using SVM and ensemble learning algorithms	Ensemble learning algorithms combined with SVM provide robust intrusion detection.	Focus on combining different ML techniques to improve detection performance.
Fang et al. [98]	Propose feature selection method for ICS using genetic algorithms	Genetic algorithms can effectively enhance feature selection for better intrusion detection performance.	Focus on enhancing security in industrial control systems through advanced feature selection techniques.
Ngo et al., [61]	Selecting and Extraction Features for Machine Learning-Based Intrusion Detection	Feature extraction more reliable, DT and MLP best for both.	ML-Based Intrusion Detection: Feature Selection and Extraction.
Talukder et al., [85]	Novel hybrid approach blending ML and DL for intrusion detection.	Accuracy of 99.99% and 100% on respective datasets.	Blending ML and DL for high accuracy intrusion detection.

Table 7
Summary of Lightweight/Compact Models Studies.

References	Purpose	Main Findings	Trend and Focus
Vo et al. [35]	Propose AI-powered IDS improving performance by enhancing training set quality	reaches higher performance in comparison to state-of-the-art techniques.	Improving dataset quality and detection accuracy, reducing latency.
Devendiran & Turukmane, [19]	Propose a deep learning-based IDS using chaotic optimization strategy	When it comes to robustness and accuracy, the Dugat-LSTM model performs better.	combining chaotic optimization techniques and DL to improve intrusion detection.
Aljehane et al. [6]	Propose a new technique for intrusion recognition and classification using deep learning	The GJOADL-IDSNS technique effectively recognizes and classifies network intrusions.	Enhancing network security using advanced optimization and deep learning techniques.
Alazzam et al. [32]	Introduce lightweight IDS with low false alarm rate	The system effectively reduces false alarms while maintaining high detection accuracy by using a combination of OCSVM and PIO.	Focus on reducing false alarms in network intrusion detection systems.
Sadhwani et al. [73]	Compact and lightweight IDS with ML classifiers.	RF achieved 100% accuracy for ToN-IoT, NB for BoT-IoT.	Developing compact and lightweight IDS models.
Khanday et al. [42]	Lightweight IDS with novel data pre-processing.	LSTM and ANN achieved 99% and 95% accuracy, respectively.	Improving accuracy of lightweight IDS with novel data pre-processing.

Table 8
Summary of Survey/Literature Review Studies.

References	Purpose	Main Findings	Trend and Focus
Mothukuri et al. [89]	An overview of the privacy and security features of federated learning	This paper examines the most recent methods in Federated learning with an emphasis on privacy and security concerns.	The study identifies key challenges and potential solutions in securing FL systems.
Valkenburg & Bongiovanni, [11]	Systematically review the application of the Three Lines Model in cybersecurity	The Three Lines Model is effective but has limitations in its application in cybersecurity.	Governance frameworks in cybersecurity.
Alsoufi et al. [56]	Review anomaly-based IDS in IoT using deep learning	Deep learning techniques are effective in dealing with security challenges in IoT ecosystems, with supervised methods performing better.	Deep learning approaches are becoming more and more popular for IoT anomaly detection, particularly after 2018.
Kumar et al. [44]	Review various IDS techniques used in network environments	Identified key trends and challenges in IDS research, with recommendations for future work.	Focus on evolving IDS techniques to address emerging network security threats.
Dasgupta et al. [18]	Review ML techniques in cybersecurity	ML techniques significantly enhance detection and response capabilities in cybersecurity.	Emphasis on the integration of ML techniques for proactive and reactive cybersecurity measures.
Khraisat et al. [2]	Review IDS techniques, datasets, and challenges	More recent and extensive datasets covering a broad range of malware activity are required.	Future IDS should address the challenge of detecting newer types of malware and overcoming evasion techniques.

quently employed, but they suffer from issues such as class imbalance, inadequate representation of certain attack types, and a focus on general IT networks rather than the distinctive features of IoT environments. This raises concerns about the generalizability of the offered intrusion detection models to genuine IoT conditions. The utilization of outdated datasets like KDDCUP'99 further complicates this, as they may not be relevant to present-day cyber threats. Additionally, the scarcity of datasets explicitly tailored for IoT settings remains an open issue. The need for datasets that accurately reflect the complexities of IoT network traffic, such as the variety of devices and communication patterns, limits the creation of effective intrusion detection systems tailored to the unique challenges of IoT environments.

Researchers are encouraged to combine more recent datasets or develop new ones to address emerging challenges because the rapid growth of attack techniques necessitates datasets that imitate the current threat landscape. Appropriate ML models in IoT security frameworks presents another set of difficulties, particularly regarding computational costs. IoT devices typically have limited resources, so deploying complex ML models on them demands careful attention to computational efficiency and energy usage. There is a need for resource-demanding model

Table 9
Summary of Datasets.

Dataset Name	Released	Provider	Advantages	Disadvantages
N-BaIot	2018	Yair Meidan and collaborators	Real-world IoT operations, emphasis on typical assaults, detect attacks from hacked IoT devices, differentiate between hour-long and millisecond-long IoT-based threats	Limited to specific IoT devices, focuses on Mirai and Bashlite DDoS attacks only.
WUSTL-IIOT2021	2021	Washington University in St. Louis.	Realistic IoT network, diverse attack types.	May require removal of certain columns for generalization, accuracy and prediction speed drop on manipulated dataset.
WUSTL-EHMS-2020,	2020.	Washington University in St. Louis.	Created using real-time Enhanced Healthcare Monitoring System (EHMS) testbed. Provides ample training samples for machine learning, ensuring excellent detection performance of ML algorithms.	Limited to healthcare monitoring systems.
NSL-KDD	Refined version of the KDD'99 dataset.	Canadian Institute for Cybersecurity at the University of New Brunswick.	No redundant or duplicate records, balanced distribution of records across different difficulty levels.	Suffers from class imbalance and overlap, lacks IoT-specific data, and does not cover all types of DDoS attacks.
ToN-IoT and BoT-IoT	2020 and 2023	School of Engineering and Information Technology, UNSW Canberra at ADFA	Realistic network environment and large-scale network designed, normal and botnet traffic, includes heterogeneous data sources.	Limited to specific IoT devices, lacks a comprehensive feature set, suffers from significant class imbalance, and does not include all DDoS attack types.
WSN-DS	2016	SEL - PSU. The Security Engineering Lab (SEL), College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia.	Specialized for WSN, it features four forms of DoS assaults. The dataset has been used in numerous machine-learning-based intrusion detection systems.	Limited to WSN, class imbalance, and dynamic network behavior issues which need to be addressed before employing this dataset for any classifier model development.
UNSW-NB / UNSW-NB15	2015	University of New South Wales (UNSW), Canberra at the Australian Defence Force Academy (ADFA)	Real modern normal and synthetic contemporary attack behaviors.	Issues with class imbalance, class overlap, cannot detect all kinds of attacks, not focused on IoT context. As new attacks arise and old attacks are evolving. DDoS attacks are not taken into consideration.
UNR-IDD	2023	The University of Nevada, Reno.	Offers network port statistics for detailed intrusion analysis, providing a diverse range of samples and scenarios for researchers.	Limited to network port statistics.
UKM-IDS20	2020	The dataset was provided by Universiti Kebangsaan Malaysia.	Includes novel attack types such as ARP Poisoning, DoS, Port Scan, and various exploits.	
SIMARGL	2021	RoEduNet, Romania.	Features derived from live traffic make the dataset highly suitable for building deployable network intrusion detection systems.[1].	This dataset serves as the basis for the multi-class classification issue.
NF-UQ-NIDS	2020	University of Queensland.	Supports the merging of multiple smaller datasets into larger, more universal NIDS datasets, encompassing flows from various network setups and diverse attack scenarios.	Prone to dimensional overload from extensive feature collection and storage, limiting the evaluation of ML model generalization.
NF-ToN-IoT	2020	The University of New South Wales (UNSW) Canberra at the Australian Defence Force Academy (ADFA).	Heterogeneous data sources, high accuracy in classifying network traffic.	ML model performance using the NF-ToN-IoT dataset is frequently inconsistent.
CICIDS / CIC-IDS2017/CSE-CIC-IDS2018	2017/2018	The Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC)1.	Offers a comprehensive set of network traffic and image representations, beneficial for network security and IDS research and development.	The datasets do not account for dynamic network changes, such as network upgrades or evolving attack techniques.
Seven CPS-specific	2022	The School of Computer Science and Informatics, De Montfort University, Leicester, UK.	Captures system behavior and interactions for AI algorithms in securing cyber-physical systems.	Datasets generated due to scarcity of real CPS datasets.
KDDCUP/KDDcup99	1999	MIT Lincoln Lab; The Defense Advanced Research Projects Agency (DARPA) as part of the Knowledge Discovery and Data Mining (KDD) Cup competition.	Publicly available and can be used for benchmarking, and comparison of different IDS, preprocessed and cleaned, suitable for supervised learning tasks.	Data is relatively old, which may not reflect modern attack techniques and is not perfectly balanced, with more normal connections than attack connections.
DS2OS	2022	University of California, Berkeley.	A large and diverse real-world IoT time series dataset that includes various data types, such as sensor data, network traffic, and system logs; well-documented and easy to use.	Unlabeled data and limited coverage of different IoT devices.
IEEE Dataport Image	2021	IEEE DataPort.	Provides a comprehensive collection of network traffic and image representations, useful for network security and IDS research and development.	Effectiveness depends on the use case, and may not cover all possible attack scenarios.

(*continued on next page*)

Table 9 (*continued*)

Dataset Name	Released	Provider	Advantages	Disadvantages
IoT-23	2020	Developed by the Avast AIC laboratory, funded by Avast Software.	Labeled dataset for IoT malware infections and benign traffic, suitable for training machine learning algorithms.	May not be sufficient for researchers who require a larger dataset, capture range may not be representative of the current IoT landscape, not diverse enough as it only contains traffic from IoT devices.
CIC-MalMem-2022	2022	The Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick.	Suitable for malware detection using ML algorithms, closely reflects real-world scenarios with prevalent malware types.	May not reflect the current malware landscape; limited diversity with only Ransomware, Spyware and Trojan Horse types.
LUFlow	2020	Lancaster University.	Continuously updated using the Citrus framework.	After downloading the dataset, certain columns need to be removed as they are unique to the attacks and would expose the type of attack to the model.
MQTT-IoT-IDS2020	2021	Hanan Hindy, Christos Tachtatzis, Robert Atkinson, Ethan Bayne, and Xavier Bellekens.	Includes generic networking scanning and MQTT brute-force attacks, suitable for ML applications; raw pcap files allow for in-depth analysis of MQTT IoT network communications and related attacks.	Requires fixing the number of features, composed of imbalanced data.

This table presents a comprehensive overview of various datasets relevant to cybersecurity, with a focus on intrusion detection and network security. Each dataset is defined by its source, purpose, and features, serving as valuable resources for researchers developing and evaluating machine learning-based solutions. The datasets range from IoT-specific to those designed for Cyber-Physical Systems (CPS) security, covering diverse attack types, network traffic scenarios, and data formats. By highlighting both the advantages and disadvantages, the table offers insights into the suitability of each dataset for different research and development needs in the dynamic field of cybersecurity.

combinations and real-world testing on IoT devices, raising issues about the adaptability and proficiency of proposed frameworks when deployed on resource-constrained IoT gadgets. The gap lies in the lack of comprehensive assessments on various IoT gadgets and datasets, restricting the versatility and flexibility of proposed intrusion recognition frameworks.

The review also points out specific challenges, including the need to balance computational efficiency with accuracy and the critical role of selecting models that suit the characteristics of the dataset. High false positive rates in anomaly-based IDS add complexity, making it difficult to differentiate between harmless anomalies and genuine attacks, which results in excessive alerts and undermines trust in the IDS.

Furthermore, a notable gap in current research is the absence of standardized evaluation metrics and benchmarks specifically tailored for IoT intrusion detection systems. Although many studies claim high accuracy rates under controlled conditions, the lack of established measures and benchmarks presents issues for comparing and generalizing these results across different contexts. Establishing evaluation standards that closely replicate real-world IoT environments is crucial for achieving more reliable assessments of intrusion detection models.

- **Dataset Imbalance and Outdated Data:** Many datasets used in IDS research, such as NSL-KDD and KDDCUP99, are outdated and exhibit significant class imbalance issues. These datasets often do not capture the latest types of attacks or the distinctive qualities of IoT environments, limiting the generalizability and effectiveness of IDS models trained on them.
- **Computational Complexity:** Integration of machine learning models into IoT security systems presents considerable challenges, particularly regarding computational costs. IoT devices are frequently resource limited, necessitating careful consideration of computing efficiency and power usage.
- **High False Positive Rates:** Anomaly-based IDS, while effective in detecting novel attacks, tend to have significant false positive rates. This occurs because of difficulty in distinguishing between benign anomalies and actual attacks, leading to unnecessary alerts and reduced trust in the IDS.
- **Lack of Real-world Testing:** Many IDS models are evaluated in controlled environments using synthetic datasets, which fail to fully represent the complexities of real-world IoT networks. More extensive real-world testing is needed to validate the performance and adaptability of these models.

6.2. Open issues

- **Feature Selection and Data Preprocessing:** Effective feature selection and data preprocessing are critical for improving IDS performance. However, there is no standardized approach for these processes in the context of IoT, leading to inconsistent results and difficulties in comparing different IDS models.
- **Standardized Evaluation Metrics:** The absence of standardized evaluation metrics and benchmarks for IoT IDS represents a critical gap in the field. Current evaluation methods vary widely, making it challenging to evaluate the relative efficacy of different IDS approaches. Developing standardized metrics that mimic real-world IoT scenarios is essential for more accurate assessments.
- **Adaptability to Evolving Threats:** IDS must be able to adjust to new and emerging attack vectors because of the dynamic nature of cyber threats. Many existing IDS models lack this adaptability, making them less effective over time. Continuous learning and updating mechanisms are required to maintain IDS relevance in the face of emerging threats.

6.3. Gap analysis

A noticeable gap in the current landscape is the limited focus on real-world applicability and the absence of standardized evaluation for IDS. Although studies claim high accuracy rates in controlled settings, real-world IoT contexts remains ambiguous. There is a need for standardized benchmarks and evaluation metrics that mimic the complexity of IoT environments, allowing for more accurate assessments of proposed intrusion detection solutions.

- **Comprehensive IoT-specific Datasets:** Many of the existing datasets struggle with severe class imbalance issues and a neglect of IoT-specific characteristics. The use of outdated datasets raises concerns about their applicability to contemporary cyber threats, and there is a scarcity of datasets designed for IoT. Developing new datasets that reflect the complexities of IoT network traffic is crucial for advancing IDS research.

Table 10
Dataset Descriptions for Cybersecurity Research.

Dataset Name	Descriptions
N-BaIot	This dataset contains real traffic data from 9 commercial IoT devices infected by BASHLITE malware and Mirai attacks. It includes 115 features covering both normal and ten types of attack traffic (e.g., Scan, Junk, UDP flooding) to evaluate intrusion detection models. The dataset captures authentic botnet traffic in a controlled environment.
WUSTL-IIOT2021	Designed for AI and ML-based research on Industrial Internet of Things (IIoT) security, this dataset includes network data representing various traffic types, such as normal, command injection, DoS, reconnaissance, and backdoor traffic, collected via an IIoT testbed.
WUSTL-EHMS-2020	Created from a testbed combining network flow metrics with patients' biometric data, this dataset addresses the scarcity of integrated biometric and network traffic datasets. It includes both normal and malicious traffic types (e.g., man-in-the-middle attacks like spoofing and data injection) and utilizes real-time data capture from medical sensors, gateways, and control components.
NSL-KDD	A refined version of the original KDD'99 dataset, it addresses several known issues with the earlier version. It consists of four major attack types: DoS, Probe, R2L, and U2R. This dataset is widely used for benchmarking intrusion detection methods and serves as a standard reference, despite not perfectly representing real-world networks.
ToN-IoT and BoT-IoT	These modern datasets are designed for AI-driven cybersecurity applications and include heterogeneous data from IoT sensors, multiple operating systems (Windows 7/10, Ubuntu 14/18), and network traffic. They are suitable for evaluating intrusion detection systems, threat intelligence, malware detection, and more.
WSN-DS	Focused on Wireless Sensor Networks (WSNs), this dataset contains 374,661 records across 17 features, which help detect and classify various Denial of Service (DoS) attacks such as Blackhole, Grayhole, Flooding, and Scheduling. The dataset uses the LEACH protocol for analysis.
UNSW-NB	This dataset comprises 2,540,044 instances of modern, realistic network activity, both normal and abnormal, including 9 types of attacks. It is commonly used for machine learning-based intrusion detection solutions and includes data sources like DNS and HTTP information.
UNR-IDD	Created to address issues like suboptimal performance and inadequate tail class representation, this dataset leverages network port statistics for fine-grained intrusion analysis. It contains 34 features that differentiate between normal data and various attack types, such as TCP-SYN, PortScan, and Overflow.
UKM-IDS20	A dataset for network intrusion detection with 46 features covering attacks like DoS, scans, ARP poisoning, and exploits. The training and test sets contain instances of both normal and malicious traffic and are analyzed using feature selection and rule-based classifiers in machine learning.
SIMARGL	Assembled from real-life network traffic, this dataset contains 44 features with an unbalanced class distribution. It is evaluated through cross-validation to provide robust security against emerging cyber threats.
NF-UQ-NIDS	A comprehensive dataset for machine-learning-based Network Intrusion Detection Systems (NIDSs), including 11,994,893 records of benign flows and various attack types (DoS, DDoS, Injection, Reconnaissance, etc.). It demonstrates the advantages of combining multiple smaller datasets into a larger, more universal one.
NF-ToN-IoT	Designed for Industry 4.0/IoT and IIoT security research, this dataset includes diverse data from IoT/IIoT sensors, multiple operating systems, and network traffic. It contains 43 features with over 16 million data rows classified as attack or benign, covering categories like DoS, DDoS, Injection, and Reconnaissance.
CIC-IDS2017	A dataset that includes benign traffic and various attack types (e.g., Brute-force, Heartbleed) across seven scenarios. It captures network traffic and system logs with 80 features extracted using CICFlowMeter-V, aimed at developing and evaluating intrusion detection systems.
Seven CPS-specific	Essential for applying AI algorithms to Cyber-Physical Systems (CPS) security, this dataset includes sensor measurements, network traffic elements, attack representations, and necessary dataset features.
KDDcup99	Based on the DARPA'98 IDS evaluation program, this dataset contains 4 GB of raw TCP dump data, processed into around 5 million connection records. It serves as a benchmark dataset for intrusion detection systems, with records labeled as normal or attack, covering DoS, U2R, R2L, and Probing categories.
DS2OS	A valuable resource for IoT time series data analysis, this dataset is large, diverse, and well-documented, covering various data types. However, it is not labeled and may not fully represent all IoT data types.
IEEE Dataport Image	Contains over 800 samples of normal and malicious traffic visualized in binary format, serving as a benchmark for intrusion detection systems. Rich visual features enhance its utility, with additional data in image format from five attack scenarios [96].
IoT-23	A labeled dataset of malicious and benign IoT network traffic, comprising twenty scenarios that represent various types of attacks on IoT networks. It includes over 760 million packets and 325 million labeled flows captured from 2018 to 2019 at the Stratosphere Laboratory.
CIC-MalMem-2022	A collection of malware memory analysis data with 58,596 records, balanced between malicious and benign memory dumps. It includes Spyware, Ransomware, and Trojan Horse malware, designed for testing obfuscated malware detection methods through memory analysis.
LUFlow	A flow-based intrusion detection dataset with robust ground truth, correlated with threat intelligence services. It contains telemetry from honeypots within Lancaster University's network and features an autonomous labeling mechanism for continuous data capture, labeling, and publishing.
MQTT-IoT-IDS2020	A simulated realistic MQTT IoT network dataset for evaluating IoT Intrusion Detection Systems. It includes various MQTT scenarios and attack data, generated using a simulated MQTT network with sensors, a broker, a camera, and an attacker. It records five scenarios: normal operation, aggressive scan, UDP scan, Sparta SSH brute-force, and MQTT brute-force attacks [41].

Table 11
Most Useful Matrices.

Metric	Description and Formula	Importance	Common Use Cases
Accuracy	Measures the proportion of true results (true positives + true negatives) in the total cases examined [5,83]. Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$	High	General performance evaluation of IDS
Precision	Measures the proportion of true positives among all positive results predicted by the IDS [65,79]. Precision = $\frac{TP}{TP+FP}$	High	Fraud detection, spam filtering
Recall	Measures the proportion of actual positives correctly identified by the IDS [65,85]. Recall = $\frac{TP}{TP+FN}$	High	Intrusion detection, medical diagnoses
F1 Score	Harmonic mean of precision and recall, useful for imbalanced datasets [15,68]. F1 Score = $2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}}$	Medium	Imbalanced datasets in machine learning
False Positive Rate (FPR)	Measures the proportion of false positives among all actual negatives [47,71]. FPR = $\frac{FP}{FP+TN}$	Medium	Medical testing, fraud detection
False Negative Rate (FNR)	Measures the proportion of false negatives among all actual positives [5,47]. FNR = $\frac{FN}{FN+TP}$	High	Security systems, risk assessment
AUC-ROC	Evaluates the performance of a binary classification system by plotting the True Positive Rate against the False Positive Rate at various threshold settings [26,50]. AUC-ROC = Area under the ROC curve	High	Classification model evaluation
Detection Rate	Measures the proportion of intrusions correctly identified by the IDS out of the total number of intrusions [83,85]. Detection Rate = $\frac{TP}{TP+FN}$	High	Intrusion detection, malware detection
False Alarm Rate	Measures the frequency of false alarms, i.e., the proportion of non-intrusive events incorrectly classified as intrusions [31,48]. False Alarm Rate = $\frac{FP}{FP+TN}$	Medium	Network security systems
Matthew's Correlation Coefficient (MCC)	Provides a balanced measure that considers all four categories of the confusion matrix (TP, TN, FP, FN) [12,17]. MCC = $\frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$	Medium	Binary classification in imbalanced datasets

Table 12
Summary of Key Findings and Conclusions from Recent Studies on IoT Intrusion Detection Systems.

Ref.	Categories	Pros:	Cons:
[96]	Method Integration for IoT Security	Real detection and classification of attacks in IoT environments, outperforming present ways on four out of five datasets.	Requires noteworthy resources due to the addition of four models. Further testing on real IoT devices and evaluations on various datasets are needed.
[73]	DDoS Attack Prevention in IoT Networks	Model commendably detects and prevents DDoS attacks in IoT networks by evaluating network patterns.	Applicability may be limited across all IoT networks. Performance depends on specific datasets, introducing variations in attack classes and data quality during training and testing.
[34]	Data Standardization for Enhanced Reliability	Offers benefits such as enhancing data reliability, precision, and applicability. Standardizes data for simpler comparison and scrutiny, rendering it more suitable for machine learning models.	
[75]	Security Improvement in Cyber-Physical Systems (CPS)	Research proposes a method to improve CPS security using a mix of machine learning approaches.	insufficiently compares machine learning techniques for CPS intrusion detection in depth.
[97]	Computational Expense Reduction in Real-Time Testing	Suggested method reduces computational expense during real-time data testing. Offers an optimal algorithm that eliminates the need for manual hyperparameter tuning calculations.	
[61]	Feature Selection vs. Extraction	Feature selection enhances detection performance and reduces training and inference time.	A drawback of feature extraction is that reducing features can lead to over-reliance on a limited set, risking compromised performance.
[91]	Strengths and Limitations of Naive Bayes Model	Naive Bayes model exhibits a low false positive rate.	Lower accuracy, evaluation of a limited number of models, and reliance on a single dataset acknowledged by the authors.
[92]	Efficient IDS Method for IoT Devices	Demonstrates superior efficiency and initial accuracy, outperforming existing techniques on three key datasets.	Validation is limited to these datasets, requiring further exploration of its effectiveness across different datasets.
[100]	Sophisticated Techniques for Data Flow Analysis	New method employs sophisticated techniques to analyze data flow and augment the quantity of less frequent samples.	Effectiveness heavily relies on the availability of a comprehensive and representative dataset.
[27]	Effective Model for IIoT Network Traffic	Model is effective in detecting harmful activities in IIoT network traffic, outperforming other methods in terms of accuracy.	Performance is best in specific intrusion detection scenarios, requires a large dataset for training, and hasn't been tested in real-world scenarios.
[93]	Machine Learning and Deep Learning for IoT Security	Recommended system employs machine learning and deep learning methodologies to improve accuracy and efficiency in detecting security threats in IoT.	Specifically designed for IoT network traffic, not applicable for real-time scenarios, and requires significant computational power.
[42]	Real-Time DDoS Attack Detection for Lightweight IoT Networks	Model excels in real-time DDoS attack detection and outperforms existing models.	Requires extensive training data, may struggle with new attack types, and is specifically designed for lightweight IoT networks.
[86]	On-Device Machine Learning for Real-Time Applications	Authors suggest using on-device machine learning for better data security in real-time applications.	Approach requires a significant amount of energy.
[57]	Evaluation of Machine Learning in IDS for IoT	Explores the application of machine learning in IDS to detect complex threats within IoT environments.	The model's effectiveness relies on feature extraction, and its real-world performance is not demonstrated, potentially varying with different datasets.
[69]	Machine Learning Challenges in Real-Time IoT Security	Authors recommend using machine learning for better data security in real-time applications.	The limited power and computational resources of IoT devices make implementing advanced security measures challenging.
[23]	Drawbacks in IoT Electric Vehicle Charging Stations (EVCSs) Security	The method incorporates with binary and multiclass models to detect a wide range of cyberattacks	Study doesn't consider deep learning, machine learning tests were done in simulation (not with a real EVCS system), and reliance only on the IoT-23 dataset may limit assessment accuracy.
[85]	Combining ML and DL for Improved Detection Rates	The method integrates ML and DL to enhance detection rates and reliability. It uses SMOTE for data balancing and XGBoost for feature selection, minimizing risks of overfitting and Type-1 or Type-2 errors.	Combining SMOTE and XGBoost also add to the computational overhead, especially when dealing with large datasets.
[43]	Advantages and Limitations of Proposed IDS System	The system provides multiple benefits, such as high accuracy, minimal false positives, and the ability to detect emerging attacks.	It demands extensive training data, lacks the ability to detect zero-day attacks, and requires regular updates.
[76]	Enhanced Accuracy with Fewer Features	Techniques enhance accuracy, lower false alarms, and achieve high accuracy with fewer features, demonstrating robustness and generalization.	Limitations include limited dataset comparisons, unexplored effectiveness of SVM and Neural Networks, and sensitivity to parameter changes in results.
[90]	Effectiveness of MLEID Method in Botnet Attacks	MLEID method effectively reduces harmful actions in botnet attacks on MQTT and HTTP protocols, surpassing traditional techniques in detection rates.	Potential downsides not specified. Model effectiveness depends on factors like training data quality and may vary in diverse IoT networks or with novel attack types, necessitating careful consideration for reliability.

- **Integration of Lightweight Models:** Integrating machine learning models into IoT security systems presents significant challenges, particularly regarding computational costs. IoT devices are often resource-constrained, making the deployment of complex ML models difficult without compromising any detection metrics. Lightweight and energy-effective IDS models that work on IoT devices with limited resources are required.
- **Holistic Evaluation Approaches:** Current research often isolates different aspects of IDS evaluation, such as accuracy, computational cost, and adaptability. A holistic approach that considers all these factors simultaneously is needed to develop truly effective IDS solutions for IoT environments. Furthermore, the absence of a unified strategy for feature selection and extraction methods is apparent in the studies. While some studies favor feature extraction over selection, others highlight the significance of particular classifiers in enhancing feature selection accuracy. A combined methodology for feature engineering would contribute to more logical and comparable research.
- **Deep Learning Techniques:** Integrating deep learning techniques and thoroughly examining their benefits and drawbacks compared to traditional machine learning models is another area that requires further exploration. Although some studies have briefly discussed the effectiveness of deep neural networks (DNNs), there is a lack of comprehensive analysis regarding their performance across diverse IoT contexts and in response to various attack vectors. While advanced algorithms such as XGBoost and AdaBoost have demonstrated significant speed, efficiency, scalability, and simplicity in detecting DDoS attacks in IoT networks, their full potential remains underexplored.
- **Privacy and Security Concerns:** Privacy and security concerns also arise from the reliance on large-scale datasets for training machine learning models, as well as the susceptibility to adversarial attacks.

Table 13
Performance Metrics and Computational Efficiency.

Metrics	Descriptions	Importance
Accuracy	Overall correctness of the IDS [45]	Evaluates the effectiveness of different models
Precision	The ratio of correctly detected malicious instances to all instances classified as malicious [88]	Assesses the IDS's ability to correctly identify malicious traffic
Recall (Sensitivity)	The percentage of malicious instances correctly detected among all actual malicious instances [29]	Determines the sensitivity of the IDS to identify all malicious traffic.
F1-Score	Harmonic mean of recall and precision [52]	Offers a balance measurement of precision and recall.
False Positive Rate (FPR)	Benign instances incorrectly classified as malicious [81]	Critical for evaluating the IDS's reliability and reducing false alarms
Training Time	Time required to train the model [14]	Crucial for timely updates and retraining of the IDS
Inference Time	required to classify new instances [101]	Essential for real-time intrusion detection
Resource Utilization	Computing resources needed for inference and training purposes [94].	Assures the IDS works in limited in resources in IoT contexts

Information security and privacy flaws in IoT networks must be addressed as a result.

The key gaps in this research can be outlined as follows:

- Numerous benchmark datasets have significant issues with class imbalance and neglect IoT-specific characteristics.
- The use of outdated datasets raises concerns about their applicability to contemporary cyber threats, and there is a scarcity of datasets tailored for IoT environments.
- Challenges exist in integrating machine learning models into IoT security systems, including resource-intensive model integrations and a lack of real-world testing on diverse IoT devices.
- Reducing computational expenses without compromising high detection accuracy is necessary, as is addressing the drawbacks of particular models, such as Naive Bayes.
- The lack of consistent evaluation criteria for Internet of Things intrusion detection systems restricts the results' ability to be compared and applied broadly.
- A unified approach for feature selection methods is missing, leading to inconsistencies in research methodologies.
- Deep learning techniques and their benefits and drawbacks, especially the performance of DNNs in diverse IoT contexts, are not fully explored.
- The effectiveness of ML algorithms like XGBoost and AdaBoost in DDoS attack detection in IoT networks needs further investigation.
- Privacy and security concerns arise from the reliance on large-scale datasets and vulnerability to adversarial attacks, posing challenges in finding novel DDoS attacks.

7. Conclusion and future directions

Internet of Things' (IoT) explosive growth has highlighted significant security challenges that necessitate advanced intrusion detection systems (IDS). This review has identified key gaps in the current IDS landscape, emphasizing the need for comprehensive IoT-specific datasets, lightweight and efficient models, and standardized evaluation metrics. Existing datasets often lack relevance to contemporary IoT environments and suffer from class imbalance, hindering the development of robust IDS solutions. Additionally, the integration of complex machine learning models into resource-constrained IoT devices poses significant computational challenges.

The reviewed studies highlight the importance of holistic evaluation approaches that consider accuracy, computational cost, and adaptability simultaneously. Moreover, while deep learning techniques offer promising results, their full potential in IoT contexts remains underexplored. Privacy and security concerns related to data reliance and vulnerability to adversarial attacks further complicate the deployment of IDS in IoT networks.

The feature engineering dilemma emphasizes the essential for a consensus on effective techniques. Future research should explore into feature selection versus extraction, proposing a homogeneous approach for researchers. Ongoing exploration is crucial, considering challenges like energy consumption in on-device machine learning and the limitations of simulated testing environments. Moreover, Future research should focus on creating comprehensive IoT-specific datasets that reflect the complexity and diversity of IoT networks, including various devices, communication patterns, and contemporary cyber threats. Optimizing lightweight, energy-efficient IDS models for implementation on IoT devices with limited resources is crucial, ensuring a balance among computational efficiency and detection accuracy. Developing standardized benchmarks and evaluation criteria that mimic real-world IoT scenarios will enable more accurate assessments and comparisons of IDS models. Adopting holistic evaluation methodologies that consider accuracy, computational cost, and adaptability, along with combining feature selection and extraction techniques into a unified framework, can enhance research coherence.

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.

CRediT authorship contribution statement

Md Mahbubur Rahman: Writing – original draft, Conceptualization, Methodology, Data curation. **Shaharia Al Shakil:** Writing – review & editing, Conceptualization, Data curation, Formal analysis, Investigation, Project administration. **Mizanur Rahman Mustakim:** Writing – review & editing, Validation, Visualization.

References

[1] S.K. Verma, A. Gupta, S.K. Bhatia, B.P. Singh, A training-resistant anomaly detection system, Computers & Security 73 (2018) 106–120, doi:10.1016/j.cose.2017.10.009.

[2] P.V.A. Khraisat, I. Gondal, J. Kamruzzaman, Survey of intrusion detection systems techniques datasets and challenges, Cybersecurity 2 (1) (2019).

[3] M. Abolfathi, S. Inturi, F. Banaei-Kashani, J. Jafarian, Toward enhancing web privacy on https traffic: a novel superlearner attack model and an efficient defense approach with adversarial examples, Comput. Secur. 139 (2023) 103673, doi:10.1016/j.cose.2023.103673.

[4] K. Ahmed, Z. Khan, Tversky loss for detecting rare network intrusions in IoT, in: Proceedings of the Network Security Conference, 2019.

[5] M. Ahmed, A.N. Mahmood, J. Hu, A survey of network anomaly detection techniques, J. Netw. Comput. Appl. 60 (2016) 19–31.

[6] N.O. Aljehane, et al., Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security, Alex. Eng. J. 86 (2024) 415–424.

[7] S. Li, et al., HDA-IDS: a hybrid dos attacks intrusion detection system for IoT by using semi-supervised CL-GAN, Expert Syst. Appl. 238 (2024), doi:10.1016/j.eswa.2024.122198.

[8] T.H. Truong, et al., Detecting cyberattacks using anomaly detection in industrial control systems: a federated learning approach, Comput. Ind. 132 (2021) 103509, doi:10.1016/j.compind.2021.103509.

[9] V. Ravi, et al., Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system, Comput. Electr. Eng. 102 (2022) 108156.

[10] A.-R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, A. Algarni, Intrusion detection in cloud computing based on time series anomalies utilizing machine learning, J. Cloud Comput. 12 (1) (2023). 127–17.

[11] I. Bongiovanni, B. Valkenburg, Unravelling the three lines model in cybersecurity: a systematic literature review, Comput. Secur. 139 (2024) 103708.

[12] P. Baldi, S. Brunak, Y. Chauvin, C.A.F. Andersen, H. Nielsen, Assessing the accuracy of prediction algorithms for classification: an overview, Bioinformatics 16 (5) (2000) 412–424.

[13] E. Brown, R. Williams, Regression techniques for anomaly detection in IoT networks, IoT J. Secur. 9 (4) (2020) 147–159.

[14] L. Brown, Training time analysis for IDS models, J. Mach. Learn. Res. 17 (1) (2023) 305–320.

[15] T. Bu, W. Zhang, L. Li, Research on network intrusion detection based on improved PSO and SVM, J. Comput. 9 (4) (2014) 827–834.

[16] L. Chen, Y. Zhao, Support vector machine-based intrusion detection in IoT networks, IoT Secur. Rev. 5 (2) (2018) 22–34.

[17] D. Chicco, G. Jurman, The advantages of the matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation, BMC Genomics 21 (1) (2020) 1–13.

[18] D. Dasgupta, Z. Akhtar, S. Sen, Machine learning in cybersecurity: a comprehensive survey, J. Def. Model. Simul. 19 (2020) 102–120, doi:10.1177/1548512920951275.

[19] R. Devendiran, A. Turukmane, Dugat-LSTM: deep learning based network intrusion detection system using chaotic optimization strategy, Expert Syst. Appl. 245 (2024), doi:10.1016/j.eswa.2024.123027.

[20] J. Doe, A. Smith, Deep learning techniques for intrusion detection in IoT networks, J. IoT Secur. 12 (3) (2020) 45–59.

[21] R. Doriguzzi-Corin, D. Siracusa, FLAD: adaptive federated learning for DDoS attack detection (2024). [Online]. Available: doi:10.1016/j.cose.2023.103597.

[22] H.W.E. Kabir, J. Hu, G. Zhuo, A novel statistical technique for intrusion detection systems, Future Gen. Comput. Syst. 79 (2018) 303–318, doi:10.1016/j.future.2017.04.001.

[23] M. ElKashlan, M.S. Elsayed, A.D. Jurcut, M.A. Azer, A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs), Electronics 12 (4) (2023) 1044, doi:10.3390/electronics12041044.

[24] E. Estopace, IDC forecasts connected IoT devices to generate 79.4ZB of data In 2025 - FutureIoT, FutureIoT (2019). Accessed: 2024-09-06, https://futureiot.tech/idc-forecasts-connected-iot-devices-to-generate-79-4zb-of-data-in-2025.

[25] W. Lee, J. Seok, E. Seo, Adversarial attack of ML-based intrusion detection system on in-vehicle system using GAN (2023) 3503–3538.

[26] T. Fawcett, An introduction to ROC analysis, Pattern Recognit. Lett. 27 (8) (2006) 861–874.

[27] T. Gaber, J.B. Awotunde, S.O. Folorunso, S.A. Ajagbe, E. Eldesouky, Industrial internet of things intrusion detection method using machine learning and optimization techniques, Wirel. Commun. Mob. Comput. 2023 (2023) 1–15, doi:10.1155/2023/3939895.

[28] T. Gates, J. Taylor, Challenges in securing the SCADA systems, Ind. Control Syst. Secur. 3 (2) (2006) 102–116.

[29] C. Glezer, Recall and sensitivity of IDS, ACM Trans. Privacy Secur. 18 (3) (2021) 7–15.

[30] J. Gu, S. Lu, An effective intrusion detection approach using svm with naïve bayes feature embedding, Comput. Secur. 103 (2021) 102158, doi:10.1016/j.cose.2021.102158.

[31] Z. Guo, Y. Ping, N. Liu, An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization, Neurocomputing 211 (2016) 78–94, doi:10.1016/j.neucom.2016.01.054.

[32] K.E. Sabri, H. Alazzam, A. Sharieh, A lightweight intelligent network intrusion detection system using OCSVM and pigeon inspired optimizer, Appl. Intell. 52 (2021) 3527–3544.

[33] T.-N. Hoang, D. Kim, Supervised contrastive resnet and transfer learning for the in-vehicle intrusion detection system, Expert Syst. Appl. 242 (2024), doi:10.1016/j.eswa.2024.123046.

[34] M.A. Hossain, M.S. Islam, Ensuring network security with a robust intrusion detection system using ensemble-based machine learning, Array 19 (2023) 100306, doi:10.1016/j.array.2023.100306.

[35] H.P. Du, H.V. Vo, H. Nguyen, APELID: Enhancing real-time intrusion detection with augmented WGAN and parallel ensemble learning, Comput. Secur. 136 (2024), doi:10.1016/j.cose.2024.103567.

[36] B. Idowu, et al., A systematic review of patient use of mobile health technologies in adult diabetes management, Health Inf. J. 24 (2) (2018) 115–129.

[37] J. Alsamiri, K. Alsubhi, Federated learning for intrusion detection systems in internet of vehicles, Future Internet 15 (403) (2023) 36–53.

[38] L. Jiang, et al., Comprehensive review of intrusion detection systems and machine learning, Cybersecur. Adv. 15 (2) (2021) 70–83.

[39] D. Maisnam, K.J. Singh, U.S. Chanu, Intrusion detection system with svm and ensemble learning algorithms, SN Comput. Sci. 4 (2023) 517, doi:10.1007/s42979-023-01954-3.

[40] M.H. Khan, A.R. Javed, Z. Iqbal, M. Asim, A.I. Awad, DivaCAN: detecting in-vehicle intrusion attacks on a controller area network using ensemble learning, Comput. Secur. 139 (2024) 103712, doi:10.1016/j.cose.2024.103712.

[41] N. Khan, F. Ali, Robust regression for intrusion detection in IoT environments (2021) 230–242.

[42] 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, doi:10.1016/j.eswa.2022.119330.

[43] A. Kumar, S. Kumar, Intrusion detection based on machine learning and statistical feature ranking techniques, IEEE (2023), doi:10.1109/confluence56041.2023.10048802.

[44] R. Kumar, P. Singh, Efficient IoT Intrusion Detection Using Binary Cross-Entropy Loss, 2021.

[45] Y. Kutlu, Overall correctness of the IDS, J. Netw. Comput. Appl. 45 (2019) 123–130.

[46] K. Lee, S. Lee, Anomaly detection in IoT using regression-based techniques, Int. J. IoT Secur. 7 (4) (2019) 123–134.

[47] W. Lee, S.J. Stolfo, A framework for constructing features and models for intrusion detection systems, ACM Trans. Inf. Syst. Secur. (TISSEC) 3 (4) (2000) 227–261.

[48] D.D. Lewis, Sequential Sampling Algorithms for Training Text Classifiers, 1994.

[49] X. Li, Y. Zhao, Auc optimization for IoT intrusion detection systems, J. Cybersecur. Metrics 5 (1) (2021) 45–58.

[50] H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, K.-Y. Tung, Intrusion detection system: a comprehensive review, J. Netw. Comput. Appl. 36 (1) (2013) 16–24.

[51] Y. Lin, S. Tan, Iou-based evaluation for IoT intrusion detection, J. Netw. Comput. Appl. 102 (2019) 81–93.

[52] M. Lundy, Balancing precision and recall: F1-score in IDS, IEEE Access 8 (2021) 135–145.

[53] M. Maddu, Y.N. Rao, Network intrusion detection and mitigation in SDN using deep learning models (2023).

[54] M. Melucci, On the trade-off between ranking effectiveness and fairness, Expert Syst. Appl. 241 (2024), doi:10.1016/j.eswa.2024.122709.

[55] N. Moustafa, et al., Holistic approach for anomaly-based intrusion detection systems, Netw. Secur. Adv. 5 (3) (2019) 45–60.

[56] M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, M. Nasser, M.A Alsoufi, S. Razak, Anomaly-based intrusion detection systems in IoT using deep learning: a systematic literature review, Appl. Sci. 11 (2021), doi:10.3390/app11188383.

[57] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, R.M.A. Mohammad, Intrusion detection system using feature extraction with machine learning algorithms in IoT, J. Sens. Actuator Netw. 12 (2) (2023) 29, doi:10.3390/jsan12020029.

[58] D. Mukhopadhyay, N. Ahuja, G. Singal, N. Kumar, Automated DDoS attack detection in software defined networking, J. Netw. Comput. Appl. 187 (2021) 103108, doi:10.1016/j.jnca.2021.103108.

[59] G. Rajeshkumar, P.V. Sagar, P. Dadheech, S.R. Dogiwal, P. Velayutham, N. Satheesh, M.V. Rathnamma, S. Sengan, Flow-based anomaly intrusion detection using machine learning model with software defined networking for openflow network, Microprocess. Microsyst. 79 (2020) 103285, doi:10.1016/j.micpro.2020.103285.

[60] V.D. Phai, Q. Shi, N. Shone, T.N. Ngoc, A deep learning approach to network intrusion detection, IEEE Trans. Emerg. Top. Comput. Intell. 2 (1) (2018) 41-50.

[61] V.-D. Ngo, T.-C. Vuong, T. Van Luong, H. Tran, Machine Learning-Based Intrusion Detection: Feature Selection Versus Feature Extraction, (Cornell University), 2023, doi:10.48550/arxiv.2307.01570.

[62] P. Nguyen, T. Le, Improving IoT Intrusion Detection with Dice Loss, 2021.

[63] Q.-V. Pham, P.K.R. Maddikunta, P. Boobalan, S.P. Ramu, T.R. Gadekallu, Fusion of federated learning and industrial internet of things: a survey, Comput. Netw. 212 (2022) 109048, doi:10.1016/j.comnet.2022.109048. [Online]. Available:

[64] M.V.P. Fazio, M. Tropea, F.D. Rango, On packet marking and markov modeling for IP traceback: a deep probabilistic and stochastic analysis, Comput. Netw. 182 (2020) 107464, doi:10.1016/j.comnet.2020.107464.

[65] S. Duttagupta, P. Krishnan, K. Achuthan, VARMAN: multi-plane security framework for software defined networks, Comput. Commun. 148 (2019) 215–239, doi:10.1016/j.comcom.2019.09.011.

[66] V. Magudeeswaran, P. Rajasekaran, Malicious attacks detection using GRU-BWFA classifier, Biomed. Signal Process. Control 79 (2023) 104219.

[67] D. Patel, M. Patel, Sparse categorical cross-entropy for IoT intrusion detection, IoT Secur. J. 6 (3) (2019) 112–125.

[68] H. Kumar, R. Singh, R.K. Singla, An intrusion detection system using network traffic profiling and online sequential extreme learning machine, Expert Syst. Appl. 42 (22) (2015) 8609-8624, doi:10.1016/j.eswa.2015.07.015.

[69] D. Rangelov, P. Lämmel, L. Brunzel, S. Borgert, P. Darius, N. Tcholtchev, M. Boerger, Towards an integrated methodology and toolchain for machine learning-based intrusion detection in urban IoT networks and platforms, Future Internet 15 (3) (2023) 98, doi:10.3390/fi15030098.

[70] Z. Rehman, I. Gondal, M. Ge, H. Dong, M. Gregory, Z. Tari, Proactive defense mechanism: enhancing IoT security through diversity-based moving target defense and cyber deception, Comput. Secur. 139 (2024) 103685, doi:10.1016/j.cose.2023.103685.

[71] R.D.-N. Kumar, S. Thakur, A. Chakraborty, R. Sarkar, Intrusion detection in cyber-physical systems using a generic and domain-specific deep autoencoder model, Comput. Electr. Eng. 91 (2021) 107044, doi:10.1016/j.compeleceng.2021.107044.

[72] D. Mohanty, S. Vadigi, K. Sethi, S.P. Das, Federated reinforcement learning based intrusion detection system using dynamic attention mechanism (2023). [Online]. Available: doi:10.1016/j.jisa.2023.103608.

[73] S. Sadhwani, B. Manibalan, R. Muthalagu, P.M. Pawar, A lightweight model for DDOS attack detection using machine learning techniques, Appl. Sci. 13 (17) (2023) 9937, doi:10.3390/app13179937.

[74] P. Sanju, Enhancing intrusion detection in IoT systems: a hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks, J. Eng. Res. 11 (2023) 356-361.

[75] V.F. Santos, C. Albuquerque, D. Passos, S.E. Quincozes, D. Mossé, Assessing machine learning techniques for intrusion detection in cyber-physical systems, Energies 16 (16) (2023) 6058, doi:10.3390/en16166058.

[76] N. Saran, N. Kesswani, A comparative study of supervised machine learning classifiers for intrusion detection in internet of things, Procedia Comput. Sci. 218 (2023) 2049–2057, doi:10.1016/j.procs.2023.01.181.

[77] V. Sarker, et al., A survey of multi-access edge computing: Definition, application, and research challenges, Edge Comput. Rev. 12 (4) (2020) 55–77.

[78] S. Sheikh, et al., Security and privacy considerations in the internet of things, IoT Secur. J. 8 (1) (2020) 15–28.

[79] J. Grover, S.K. Gupta, M. Tripathi, Hybrid optimization and deep learning based intrusion detection system, Comput. Electr. Eng. 100 (2022) 107876.

[80] A. Smith, J. Doe, Using focal loss to handle imbalance in IoT intrusion detection, Cybersecur. Adv. 15 (2) (2020) 70–83.

[81] A. Smith, B. Jones, Evaluating the false positive rate in IDS, Int. J. Netw. Secur. 20 (2) (2022) 75–85.

[82] S. Srinivas Akkepalli, Anomaly-based network intrusion detection using hybrid CNN, Bi-LSTM deep learning techniques (2024) 0950–0958.

[83] R. Dara, S.C. Hamed, S.C. Kremer, Network intrusion detection system based on recursive feature addition and bigram technique, Comput. Secur. 73 (2018) 152–166, doi:10.1016/j.cose.2017.10.011.

[84] Y. Shiraishi, T.T. Thein, M. Morii, Personalized federated learning-based intrusion detection system: poisoning attack and defense (2024). [Online]. Available: doi:10.1016/j.future.2023.10.005.

[85] M.A. Talukder, K.F. Hasan, M.M. Islam, M.A. Uddin, A. Akhter, M.A. Yousuf, F. Alharbi, M.A. Moni, A dependable hybrid machine learning model for network intrusion detection, J. Inf. Secur. Appl. 72 (2023) 103405, doi:10.1016/j.jisa.2022.103405.

[86] N. Tekin, A. Acar, A. Ariş, A.S. Uluagac, V. Güngör, Energy consumption of on-device machine learning models for IoT intrusion detection, Internet Things 21 (2023) 100670, doi:10.1016/j.iot.2022.100670.

[87] S. Thomas, M. Green, Multi-label classification in IoT intrusion detection using hamming loss, IoT Secur. Privacy 3 (1) (2018) 45–56.

[88] E. Tsai, Precision in intrusion detection systems, IEEE Trans. Inf. Forensics Secur. 14 (5) (2020) 1012–1023.

[89] S. Pouriyeh, V. Mothukuri, R.M. Parizi, Y. Huang, A Survey on Security and Privacy of Federated Learning, Elsevier B.V., 2021, doi:10.1016/j.future.2020.10.007. [Online]. Available:

[90] S. Vanitha, P. Balasubramanie, Improved AnT colony optimization and machine learning based ensemble Intrusion Detection model, Intell. Autom. Soft Comput. 36 (1) (2023) 849–864, doi:10.32604/iasc.2023.032324.

[91] E.K. Viegas, A.O. Santin, P. Tedeschi, Toward a reliable evaluation of machine learning schemes for network-based intrusion detection, IEEE Internet Things Mag. 6 (2) (2023) 70–75, doi:10.1109/iotm.001.2300106.

[92] M. Vishwakarma, N. Kesswani, A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection, Decis. Anal. J. 7 (2023) 100233, doi:10.1016/j.dajour.2023.100233.

[93] A.J. Wadate, S. Deshpande, Edge-based intrusion detection using machine learning over the IoT network, IEEE (2023), doi:10.1109/icetet-sip58143.2023.10151535.

[94] P. Wang, Resource utilization in ids for IoT environments, IEEE Trans. Comput. 67 (11) (2023) 145–158.

[95] J. White, P. Black, Optimizing cohen's kappa for intrusion detection in IoT, J. IoT Cybersecur. 6 (2) (2018) 89–101.

[96] B. Xu, L. Sun, X. Mao, R. Ding, C. Li, IoT intrusion detection system based on machine learning, Electronics 12 (20) (2023) 4289, doi:10.3390/electronics12204289.

[97] H. Xu, Z. Sun, Y. Cao, H. Bilal, A data-driven approach for intrusion and anomaly detection using automated machine learning for the internet of things, Soft Comput. 27 (19) (2023) 14469–14481, doi:10.1007/s00500-023-09037-4.

[98] X. Lin, J. Wang, H. Zhai, Y. Fang, Y. Yao, A feature selection based on genetic algorithm for intrusion detection of industrial control systems, Comput. Secur. 139 (2024) 103708.

[99] L. Hu, Z. Zhang, Z. Wu, J. Wang, H. Wu, A network intrusion detection method based on semantic re-encoding and deep learning, J. Netw. Comput. Appl. 164 (2020), doi:10.1016/j.jnca.2020.102688.

[100] M. Zakariah, S.A. AlQahtani, M. Al-Rakhami, Machine learning-based adaptive synthetic sampling technique for intrusion detection, Appl. Sci. 13 (11) (2023) 6504, doi:10.3390/app13116504.

[101] J. Zhang, Real-time intrusion detection: inference time considerations, IEEE Internet Things J. 9 (4) (2023) 255–265.

[102] X. Zhang, H. Wang, Kl divergence for anomaly detection in IoT networks, IEEE Trans. Inf. Forensics Secur. 16 (2021) 1302–1314.

[103] P. Zhu, Z. Fan, S. Guo, K. Tang, X. Li, Improving adversarial transferability through hybrid augmentation, Comput. Secur. 139(2024) 103674. doi:10.1016/j.cose.2023.103674.