electronics

MDPI

Review

Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review

Mujaheed Abdullahi [1,*], Yahia Baashar [2,*], Hitham Alhussian [1], Ayed Alwadain [3], Norshakirah Aziz [1], Luiz Fernando Capretz [4] and Said Jadid Abdulkadir [1]

[1] Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Malaysia; seddig.alhussian@utp.edu.my (H.A.); norshakirah.aziz@utp.edu.my (N.A.); saidjadid.a@utp.edu.my (S.J.A.)
[2] Institute of Sustainable Energy (ISE), Universiti Tenaga Nasional (UNITEN), Kajang 43000, Malaysia
[3] Computer Science Department, Community College, King Saud University, Riyadh 145111, Saudi Arabia; aalwadain@ksu.edu.sa
[4] Department of Electrical & Computer Engineering, Western University, London, ON N6A5B9, Canada; lcapretz@uwo.ca
* Correspondence: abdullahi_18001208@utp.edu.my (M.A.); yahia.baashar@uniten.edu.my (Y.B.)

Abstract: In recent years, technology has advanced to the fourth industrial revolution (Industry 4.0), where the Internet of things (IoTs), fog computing, computer security, and cyberattacks have evolved exponentially on a large scale. The rapid development of IoT devices and networks in various forms generate enormous amounts of data which in turn demand careful authentication and security. Artificial intelligence (AI) is considered one of the most promising methods for addressing cybersecurity threats and providing security. In this study, we present a systematic literature review (SLR) that categorize, map and survey the existing literature on AI methods used to detect cybersecurity attacks in the IoT environment. The scope of this SLR includes an in-depth investigation on most AI trending techniques in cybersecurity and state-of-art solutions. A systematic search was performed on various electronic databases (SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI). Out of the identified records, 80 studies published between 2016 and 2021 were selected, surveyed and carefully assessed. This review has explored deep learning (DL) and machine learning (ML) techniques used in IoT security, and their effectiveness in detecting attacks. However, several studies have proposed smart intrusion detection systems (IDS) with intelligent architectural frameworks using AI to overcome the existing security and privacy challenges. It is found that support vector machines (SVM) and random forest (RF) are among the most used methods, due to high accuracy detection another reason may be efficient memory. In addition, other methods also provide better performance such as extreme gradient boosting (XGBoost), neural networks (NN) and recurrent neural networks (RNN). This analysis also provides an insight into the AI roadmap to detect threats based on attack categories. Finally, we present recommendations for potential future investigations.

Keywords: systematic literature review; internet of things; artificial intelligence; machine learning; deep learning; intrusion detection systems; cybersecurity; cyberattacks

Citation: Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics* **2022**, *11*, 198. https://doi.org/10.3390/electronics11020198

Academic Editor: Qusay H. Mahmoud

Received: 29 October 2021
Accepted: 4 December 2021
Published: 10 January 2022

1. Introduction

The large-scale growth of the Internet of things (IoT) in recent years has contributed to a significant increase in fog computing, smart cities, and Industry 4.0, all of which execute the complex data processing of confidential information that must be protected against cybersecurity attacks. Cybersecurity attacks have increased rapidly in various domains, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes [1]. As a result of their wide range of services, IoT device sensors generate large amounts of data that requires authentication, security, and privacy. Previously, traditional methods and frameworks were used to ensure the security of IoT. However, the application

of different artificial intelligence (AI) methods for detecting cybersecurity attacks has gained in popularity over the years.

IoT comprises interconnected devices that are increasingly developed on a large scale, taking into account various characteristics through cloud and fog computing, where the processing of real-time applications can be enhanced [2]. Cyber-physical systems (CPSs) are integrated technologies such as healthcare IoT, industrial IoT (IIoT), smart cities IoT, AI and big data, that are part of the fourth industrial revolution (Industry 4.0), and are used for innovation in smart industries to promote data transmission between networks [3,4]. To overcome the security issues that threaten the IoT, several researchers have developed IDSs based on various AI approaches. Kurte et al. [5], for example, introduced a distributed service framework that supports the development of trustworthiness and privacy protection for multidirectional data aggregation for edge computing enhancement [6]. Diro and Chilamkurti [7] proposed a detection system using deep learning (DL) methods to detect cybersecurity attacks in IoT. They compared the DL model with traditional machine learning (ML) approaches. Farivar et al. [8] identified AI for the detection of malicious attacks in CPS and IIoT and proposed a hybrid intelligent classic control approach for the reconstruction of cyberattacks on the input data of non-linear CPS through shared networks.

Security in the IoT requires additional considerations to protect connected smart devices from threats and other vulnerabilities using effective AI techniques towards monitoring [9–11]. In addition, IoT security systems are designed using AI enhanced encryption algorithms to archive privacy [12,13]. For example, Obaidat et al. [14] investigated in-depth IoT attacks, threats and vulnerability through classification based on severity impact, also providing a multi-faceted method to countermeasure those security concerns. Li et al. [15] proposed a novel privacy prevention of ML training with classification process through a security framework based on a homomorphic encryption scheme over a matrix ring, which also supports ciphertexts homomorphic comparison. Sarica and Angin [16] provided explainable security in IoT networks by proposing a real-time automated intrusion detection approach using ML classifiers in software-defined networking (SDN) application layer to detect an attack. Aleem et al. [17] provide security concerns for data warehouse (DWH) with each type of security approach. Furthermore, it includes a new and unique CPS if the countermeasure is insufficient [18]. Patil et al. [19] proposed a virtual machine-assisted lightweight agent-based malware detection framework for securing a virtual machine in cloud computing, while, Dang et al. [20] proposed an authentication method for securing cloud servers in IoT environments. In addition, Moustafa [21] proposed a new IoT network distributed architecture using an AI-based security system.

Owing to their IDSs, AI methods are widely used for providing security to IoT devices and networks to overcome the challenges, security issues and abnormalities [22]. Recent studies by Ghosh et al. [23] claimed that the application of AI in IoT is a breakthrough for reducing human effort in providing security. More recent evidence was reported by Bland et al. [24]; they proposed ML cyberattack and defense strategies using reinforcement learning algorithms to improve the ability to detect cybersecurity attacks. Rathore and Park [25] used a semi-supervised learning-based distribution attack detection framework for IoT, where they introduced a fog-based attack detection framework and proposed an extreme learning machine (ELM)-based semi-supervised fuzzy method to achieve adequate generalization performance at a fast detection rate. Kasongo and Sun [26] adopted a DL method and developed an approach for wireless IDS using wrapper-based feature extraction for wireless networks based on a feed-forward deep neural network.

However, certain limitations exist because the use of AI in cybersecurity detection introduces considerable exposure to IoT devices and networks. In addition to the development of IoT, several centralized attack detection mechanisms have been proposed to detect attacks in the IoT using a supervised ML algorithm. In spite of this, these mechanisms have failed to achieve significant results because of the distinct requirements of devices, such as scalability and distribution, [25]. However, there's a need for IoT security guidelines to evaluate the existing methods [27]. Previous systematic reviews have made significant

contributions to the cybersecurity field. The work of [28] investigated and analyzed the importance of artificial immune systems in IoT environments by evaluating and identifying the performance of empirical research on the approaches to secure IoT environments.

In this review, we intend to explore and analyze both ML and DL methods used for the detection of cybersecurity attacks in IoT devices and networks by formulating and addressing research questions, and filling the current research gaps in the area of IoT security by attempting to overcome limitations in the existing work.

IDSs, particularly those designed using AI such as anomaly-based, are preferred for detecting cybersecurity attacks in mobile devices with integrity verification schemes for cloud storage in an endpoint environment [2,29–31]. In this study, we analyze the research published on IoT security and identify the best possible solutions under different scenarios, including detection algorithms, frameworks, architectures, and models. Previously, artificial immune systems have been reviewed to secure IoT via fog orchestration [28,32–34]. Herein, we mapped the literature to identify past learnings and discuss potential future scenarios. To this end, we formulated three research questions.

This SLR (systematic literature review) consists of ten sections and is organized as follows. Section 1 introduction, Section 2 provides metasurvey, Section 3 presents survey methodology, Section 4 presents results, Section 5 presents SLR major findings based on the research questions, Section 6 presents artificial intelligence roadmap, Section 7 presents a discussion, Section 8 presents limitations of the study, Section 9 presents recommendations for future investigations and Section 10 is the conclusion.

1.1. Huge Network Traffic Dataset and Imbalanced Dataset

IoT IDSs using AI have challenges of the huge amount of datasets from network traffic which leads to high false alarm and low detection rates [35]. This can be addressed using feature reduction technique. Singh et al. [35] proposed a technique for IDS based on online sequential extreme ML which profiling less time complexity while irrelevant features are excluded using correlation, consistency feature selection. Figure 1 show data imbalanced problem from multi-classes relationship between more complex and classes. In addition, the ML IDSs face challenges due to imbalanced datasets when processing/training entire data, while this can be addressed by identification of intrusion through network traffic behavior and reassembling imbalanced datasets.

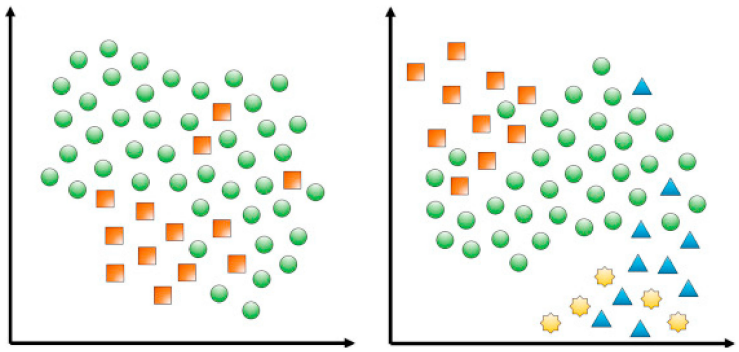

Figure 1. Two possible class imbalance scenarios: (**left**) binary imbalanced problem and (**right**) multi-class imbalanced problem [36].

1.2. Research Contribution

Several research studies address the importance of AI in IoT cybersecurity. In this study, we investigate the use of AI methods in the detection of a cybersecurity attack in the IoT. The research contribution for this SLR includes the following:

- We formulate and answer three research questions using existing empirical studies that use AI methods in IoT.

- We review the current uses of AI methods in detecting IoT threats by evaluating the approach using datasets.
- We present a classification of studies based on ML Algorithms, DL algorithms, model performance, IDSs and types of threats.
- We also discuss the limitations of the study and recommendations for future studies.

2. Metasurvey

In this section, related works have been reviewed based on literature review studies. The existing studies related to AI algorithm-based technique has been used to detect cyber-attacks and anomaly activities in IoT nowadays, through developing smart, secure and provide, IoT infrastructure which can detect the abnormal, vulnerability from cyber-attack automatically, the ML, DL algorithms was the best to protect the systems than normal traditional method when it is in an abnormal state. For such reason, the goal is to identify what are the most effective AI methods to detect an attack, threats in IoT environment and investigate the available practice to reduce those attacks using effective techniques. In addition, IoT is subjected to serious risk of cyber security attack due to its huge amount of data generated through the network and communication layers of field devices such as sensor data and actuators which are usually used for real-time monitoring and predictions.

Ahmad et al. [37] conducted a comprehensive analysis of different DL models which include CNN, RNN, LSTM using IoT-Botnet 2020 dataset to propose an efficient anomaly detection using mutual information (MI) by considering deep neural network (DNN) for an IoT network. Similar study by Ali and Choi [38] presents a comprehensive review on state-of-art AI techniques for distributed smart grids with aims to support the integration of renewable energy resources security. Tahsien et al. [39] present a survey of ML-based solutions for IoT security in terms of different types of possible attacks. Alsoufi et al. [40] present a review analysis on anomaly-based intrusion detection systems in IoT using several DL techniques. Echeverría et al. [41] investigated in-depth on cybersecurity model based on hardening to secure IoT using a model of sequence consist seven steps to minimize the attack surface through executing hardening processing. However, new concern about cybersecurity issues are rising in IoT infrastructure Djenna et al. [42] presents a critical analysis of the most recent cybersecurity issues for IoT-based critical infrastructures. Another progressive research on IoT security by Mahbub [43] presents an exhaustive analysis based on perspective protocols, vulnerabilities and preemptive architectonics.

This review focuses on AI techniques used between 2016 and 2021. However, before 2016, AI has played a role in cybersecurity. The dominant techniques during this time include genetic algorithms, fuzzy logic and neural networks where many researchers proposed IDSs and intelligence architecture frameworks based on AI. For example, in 2015, Dilek et al. [44] provided a comprehensive review on AI techniques to combat cybercrimes with efficient methods for detecting and preventing cyber-attacks. In addition, Greensmith [45] provided how artificial immune systems (AIS) can maintain and secure IoT networks using advanced AIS. Moreover, the authors provide its challenges and limitations. In 2011, Morel [46] provided a broad overview of AI as a feature of cybersecurity based on its different approaches.

Table 1 shows comparison details of other related studies in the area. The systematic review provides an in-depth analysis with future recommendations towards cybersecurity detection in IoT using AI techniques.

Table 1. Comparison of other related studies in the area: (√: Yes, x: No).

Authors	Year	IoT	IoT Security	Systematic Study	DL Technique	ML Technique
Obaidat et al. [14]	2020	√	√	√	x	x
Mohanta et al. [47]	2020	√	√	x	x	√
Sharma et al. [48]	2020	x	x	√	x	√
Alsoufi et al. [49]	2021	√	√	x	√	x
Haji & Ameen [50]	2021	√	√	x	x	√
Aversano et al. [51]	2021	√	√	√	√	x
Istiaque et al. [52]	2021	√	√	x	x	√
Rjab & Mellouli [53]	2021	√	√	x	√	√
Tsiknas et al. [54]	2021	√	√	x	x	x
Our study	2021	√	√	√	√	√

3. Survey Methodology

The current systematic literature review was conducted based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [55]. The standard guidelines by Kitchenham [56] were applied, while Figure 2 illustrate the study screening and selection process. Table 2 illustrates the SLR method.

Table 2. SLR method based on PRISMA protocol.

Title	Description
Abstract	Provides an overview of the study which includes a background of research, methodology and findings
Introduction	Provides an overview of existing knowledge related to IoT, IoT security and AI
Methodology	Research question Information source and database Search strategy and key terms Eligibility criteria Quality assessment Data extraction
Result Discussion	Provides the finding based on result analyses for the study
Conclusion	Provide conclude outcomes of the entire research study

3.1. Research Motivations

The approach to detect cybersecurity attacks in IoT using AI is widely developing. Due to this, there's need to explore in-depth analyses through examining previous studies. Our study goal is to identify what are the most effective AI methods to detect attacks, threats in IoT systems and investigate the available practice to reduce those attacks using effective techniques. For this purpose, readers will have an idea about IoT security using AI especially those new in the area. Some studies focused on traditional methods, while some focused on DL techniques for IoT security. In our study, we explore both ML and DL techniques for IoT security with feature recommendations. In addition, we focused on related studies to IoT security using AI methods.

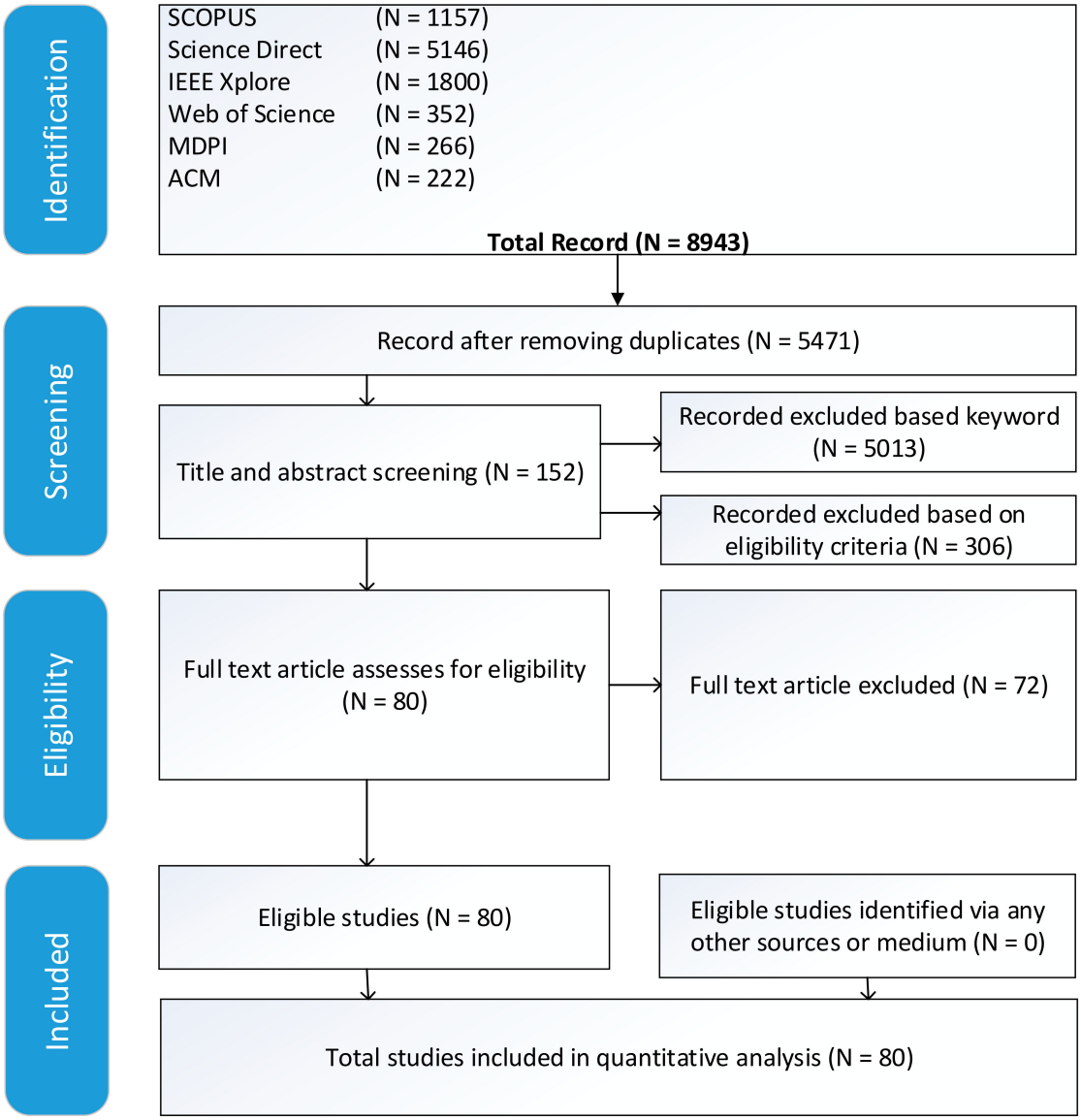

Figure 2. PRISMA flow diagram of studies' screening and selection.

3.2. Research Question

RQ1: What are the existing cybersecurity attacks and threats in the IoT environment?

RQ2: What are the common AI methods used to detect cybersecurity attacks in the IoT?

RQ3: What are the available practices to reduce cybersecurity attacks for IoT using AI approaches?

3.3. Information Sources and Database

The literature search was performed using different database sources based on a search strategy developed to identify the relevant studies. To this end, a systematic computerized search was finalized using three database sources, namely SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI. We developed a search strategy to identify relevant literature following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines during all stages [55]. Figure 2 presents the article screening and selection processes which were assessed by two authors of this study (M.A. and Y.B.).

3.4. Search Strategy and Key Terms

The search strategy was customized for three databases using the following search terms: 'Artificial Intelligence' OR 'Machine Learning' OR 'Deep Learning' OR 'AI' OR 'ML' OR 'DL' AND 'Cybersecurity' OR 'Attacks' OR 'Threats' AND 'IoT' OR 'CPS' 'Industrial IoT' OR 'Medical IoT' OR 'Energy IoT' AND 'Detection' OR 'Prediction' OR 'Identification' OR 'Detect'. All searches spanned the period from the inception of the database until 2021 and included journal articles with a few review papers published only in English.

3.5. Eligibility Criteria

The search was primarily focused on the mapping of existing literature on Internet security and ML security in the fields of computer science, decision science, and mathematics. The search covered the years 2016 to 2021; all articles published before 2016 were excluded from the search. Moreover, the search was performed on a global level and not restricted to a specific country or region. At this stage, 72 research articles were excluded, and the 80 selected research articles were extracted. Table 3 summarizes the inclusion and exclusion criteria used in selecting the research articles.

Table 3. Inclusion and exclusion criteria.

	Inclusion	Exclusion
Types of study	Original and review articles.	Thesis, white papers, communication letters, reports and editorials.
Source	Peer-reviewed and conference proceedings.	-
Publication year	January 2016–2021.	Pre 2016–Post September 2021.
Language	English.	Non-English.
Region	Not restricted to a particular region	-
Intervention	ML and DL methods.	Traditional and statistical methods.
Settings	Cybersecurity threats in IoT devices and networks.	Non IoT settings

3.6. Quality Assessment

Quality assessment was based on original research and a few review articles. To maintain the quality of the review, all duplicate records were thoroughly checked. In particular, the abstracts of all research articles included in the review process were checked in detail and filtered to ensure their quality and relevance. A careful evaluation of each research paper was performed at a later stage. Another exclusion criterion was to limit the articles to those published in the English language. Consequently, six articles in non-English languages were excluded from the study.

3.7. Data Extraction

Selected studies were placed into a data extraction spreadsheet using Microsoft Excel 2019. The data extracted from the studies were: author(s), year, AI type, algorithm used, performance focus, model performance, number of predictive features, types of cybersecurity attacks and data sources. The data extraction was performed by two authors of this study (N.A. and S.J.A).

4. Results

In this section, we summarize the results of the screening and search processes based on the PRISMA guidelines. First, we describe the characteristics of selected research studies by presenting their data quantitatively, which includes listing documents by year, journal sources, subject area, and the algorithm used. Second, we classify the literature of selected studies using the AI method, model performance, and types of attacks. The analysis of all results discussed in this section is directly related to the research questions of this study.

4.1. Characteristics of the Selected Studies

Figure 3 depicts the yearly distribution of the studies from 2016 to 2021. It was observed that the number of studies has significantly increased over the years, which signifies that the field of cybersecurity and IoT are gaining in popularity and receiving increasing attention from various scholars. The findings also indicate that AI models have produced satisfactory results in detecting IoT cybersecurity threats. As seen in Figure 3, the highest number of studies were published in 2020 (N = 29, 52.7%), followed by 2019 (N = 11, 20%).

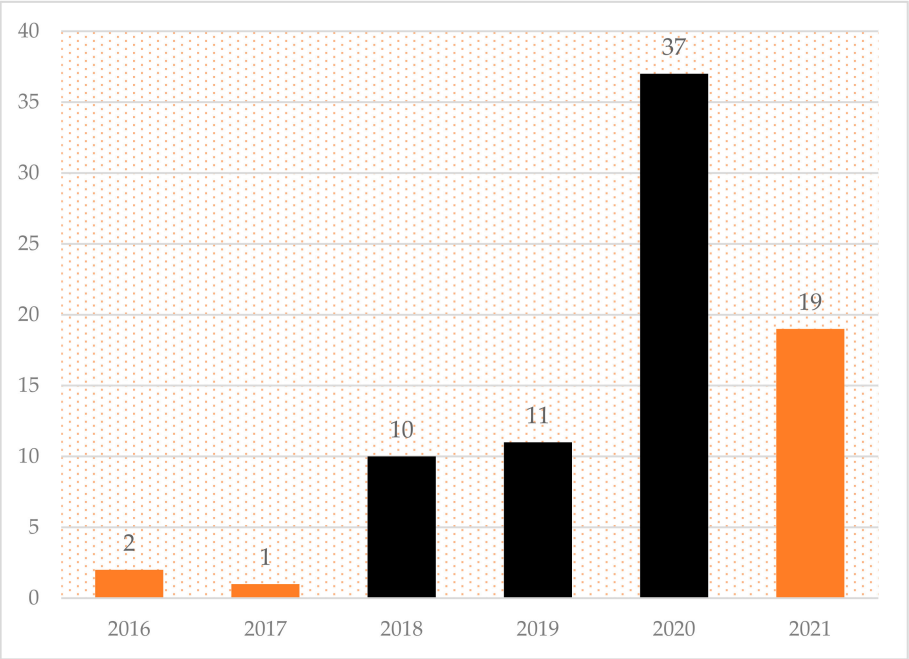

Figure 3. Distribution of studies based on the year of publication.

Figure 4 illustrates the distribution of our search results by journal sources, including *IEEE Access, IEEE Internet of Things Journal, Future Generation Computer Systems, IEEE Transactions on Industrial Informatics, Journal of Network and Computer Applications, International Journal of Information Management*, Ad Hoc *Networks, Asian Journal of Research in Computer Science, Journal of Cloud Computing, Applied Soft Computing, Computers & Security, Computer Science Review, Journal of Information Security and Applications, Sustainable Cities and Society, International Journal of Information Security, Enterprise Information Systems, Additive Manufacturing, Journal of Systems Architecture, Simulation Modelling Practice and Theory, Measurement, Microprocessors and Microsystems, Internet of Things, Expert Systems with Applications, Journal of ISMAC, MPDI Sensors, MPDI Electronics, MDPI Applied Sciences, International Journal of Environmental Research, Information Sciences* and *Public Health, and Journal of Ambient Intelligence and Humanized Computing*. This result shows that the studies are obtained from respected scholarly journals.

Figure 5 depicts the distribution of the selected studies in terms of subject areas. The highest percentage of studies was found in the field of computer science (32%), followed by decision science (16%), which was followed by engineering (14%), material science (13%), others (11%), mathematics (9%) and energy (5%). This indicates that in comparison with other fields of study, computer science has performed more investigation of the use of AI methods for IoT cybersecurity threats.

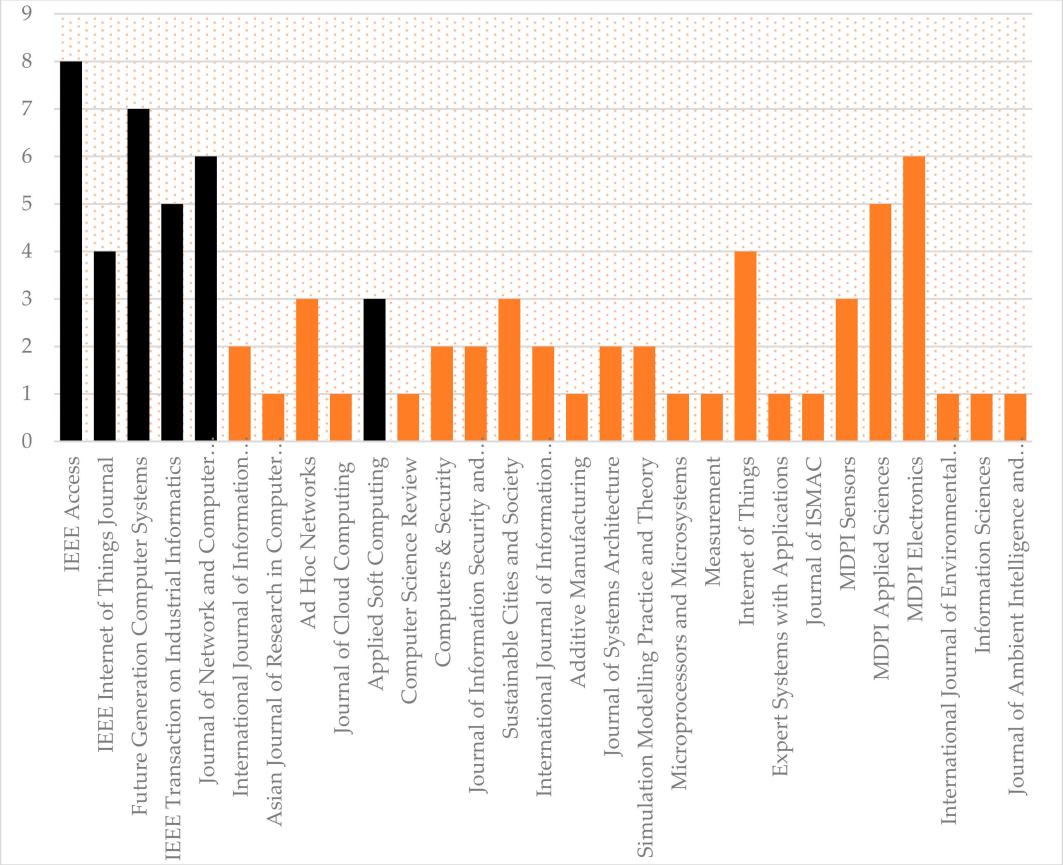

Figure 4. Distribution of studies based on the journals.

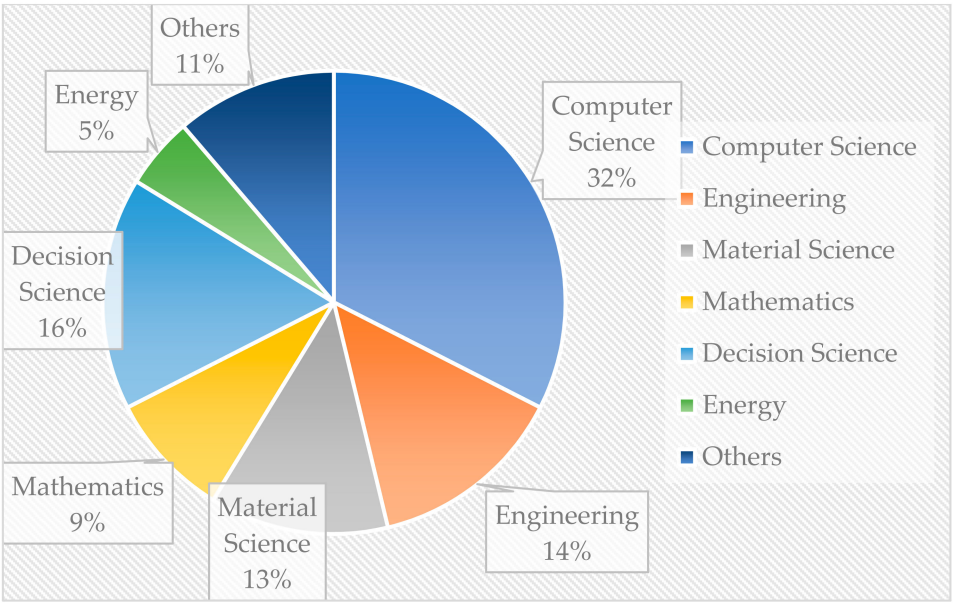

Figure 5. Distribution of the studies in terms of subject areas.

Figure 6 illustrates the characteristics of the selected studies that examined the implementation of different AI algorithms in detecting threats to the IoT. These algorithms are naïve Bayes (NB), decision tree (DT), random forest (RF), support vector machine (SVM), support vector regression (SVR), k-nearest neighbors algorithm (k-NN), fuzzy pattern tree (FPT), fuzzy C-means algorithm, logistic regression (LR), deep learning (DL), and artificial neural network

(ANN). The results indicate that 15 studies used DL algorithms, 34 studies used various ML algorithms, and other studies focused on the current issues related to IoT security.

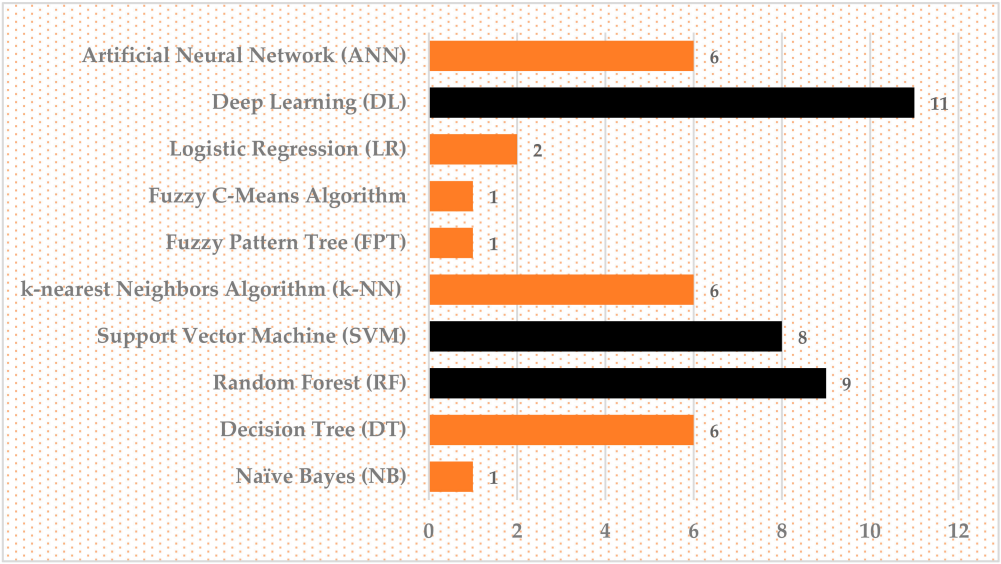

Figure 6. Characteristics of studies based on AI methods.

4.2. Classification of Selected Studies

4.2.1. Summary of Studies Classified Based on ML Algorithms

Table 4 summarizes the classification of the studies based on ML algorithms used in the detection of IoT threats. The table includes article authors, year, description of their work, datasets, and ML algorithms used. ML methods are the most promising for ensuring security within the IoT environment, whereas framework models, IDSs, techniques, and intelligent architectures have been proposed by various researchers to detect threats and attacks in IoT devices and fog-based systems. According to the summary of studies, SVM, SVR, DT, RF, NB classifier, LR, KNN, and fuzzy algorithms are commonly used to address cybersecurity-related issues. The ML algorithms were categorized into supervised, unsupervised, and semi-supervised learning-based methods. Furthermore, certain studies combined different methods to compare their performances, which are referred to as intelligent hybrid models.

4.2.2. Summary of Studies Classified Based on DL Algorithms

Table 5 summarizes the classification of the studies based on the DL algorithms used in the detection. The table includes article authors, year, description, datasets, and DL algorithms used. DL is a subsection of ML that is based on a neural network and plays a vital role in cybersecurity within the IoT environment. Most researchers have proposed smart IDSs, framework models, techniques, intelligent architectures, and fog-based methods to detect threats in the identification systems of IoT devices and networks. According to the selected studies, most researchers used deep autoencoders (DA), recurrent neural networks (RNN), convolutional neural networks (CNN), deep neural networks (DNN), multi-layer perception neural networks, and deep belief networks (DBN) to address cybersecurity issues. Certain studies combined different DL models to compare their performances, which are referred to as hybrid models. Additionally, most studies' datasets are KDD, which has limitations due to it being outdated in the IDS community.

Table 4. Summary of studies classified based on ML algorithms.

Author	Yeah	Description	Dataset	ML Algorithm
Shafiq et al. [57]	2020	To overcome the challenge of ML algorithms for cyber-attacks, a new framework model and a hybrid algorithm were proposed where the BoT-IoT identification dataset is used, to determine which ML algorithm is more effective.	Bot-IoT dataset	NB, BayesNet, DT, RF
Rahman et al. [58]	2020	To address the limitations of centralized IDS for resource-constrained devices, this work proposes two techniques, semi-distributed and distributed, that combine high-performance feature extraction and selection with potential fog-edge coordinated analytics.	AWID dataset	SVM
Roldán et al. [59]	2020	Proposes an intelligent architecture that integrates CEP and Machine Learning (ML) to identify different types of IoT security attacks in real-time. Such an architecture in particular, is capable of conveniently managing event patterns whose conditions are dependent on values obtained by ML algorithms.	MQTT regular traffic packets	SVR
Li et al. [60]	2020	This work analyzes the performance of DAS-CIDS in the areas of detection and false alarm reduction using both datasets in real network scenarios.	KDD99	KNN, SVM, RF, DT
Dovom et al. [61]	2019	For malware identification and categorization, transforms the programs' OpCodes into a vector space and uses fuzzy and fast fuzzy pattern tree algorithms in IoT.	IoT, Vx-Heaven, Kaggle and Ransomware	Fuzzy Pattern Tree (FPT)
Rathore & Park [25]	2018	Provides a fog-based attack detection system based on the fog computing paradigm and a new ELM-based Semi-supervised Fuzzy C-Means (ESFCM) approach.	NSL-KDD	Fuzzy C-Means Algorithm
Wang et al. [62]	2019	Proposes ML-based attack detection model for power systems that can be trained using data and logs gathered by phasor measuring units (PMUs).	Industrial Control System (ICS) cyber-attack datasets	KNN, SVM, DT, RF, XGBoost
Hasan et al. [63]	2019	Anomaly and attack detection in IoT sensor data were compared using multiple ML models.	Kaggle, Message Queuing Telemetry Transport (MQTT) protocol.	LR, SVM, DT, RF
Bhatia et al. [64]	2019	For securing IoT environments, the authors propose a network-centric, behaviour-learning-based anomaly detection solution, where predictability of TCP traffic from IoT devices can be used to detect various types of DDoS attacks in real-time using unsupervised machine learning.	IoT traffic	SVM
Doshi et al. [65]	2018	Demonstrate how highly accurate DDoS detection can arise in IoT network traffic using IoT-specific network behaviours.	Simulation of consumer IoT device network	KNN, SVM, DT, RF
An & Liu, [66]	2019	This work modelled two types of cyber-attacks (e.g., transitory and steady cyber-attacks). A multivariate Gaussian-based anomaly detection method is suggested to detect these false data injections more effectively.	Simulated data	K-means clustering, Linear Regression

Table 4. *Cont.*

Author	Yeah	Description	Dataset	ML Algorithm
Alrashdi et al. [67]	2019	Proposes a system for the IoT Anomaly Detection, which is a smart anomaly detection based on the Random Forest algorithm.	UNSW-NB 15	Random Forest
Azmoodeh et al. [68]	2018	Presents an approach based on ML to detect ransomware threats through monitoring the android device power consumption.	Ransomware samples from Android applications	KNN, SVM, RF
Soe et al. [69]	2020	Proposes a novel function selection methodology, known as the correlated set gain-ratio (CST-GR) threshold, to choose proper functionality to build a lightweight IDS based on machines using a new feature selection algorithm.	Bot-IoT dataset from Cyber Range Lab	Logistic Model Tree, RF
Rashid et al. [70]	2020	This work explores an approach for attack and anomaly detection based on algorithms for the defense and mitigation of IoT cybersecurity risks in a smart city.	UNSW-NB15, CICIDS2017	SVM, DT, RF, KNN

Table 5. Summary of studies classified based on DL algorithms.

Author	Yeah	Description	Dataset	DL Algorithm
Haddadpajouh et al. [71]	2018	Investigates the potential of RNN models in detecting IoT malware.	IoT application dataset	RNN
Diro and Chilamkurti, [7]	2018	A new method for cybersecurity attack detection using a deep learning method in the social IoT was investigated. This work also compared different DL and ML models.	KDDCUP99, ISCX, NSL-KDD	Deep Learning Model
G and Selvakumar, [72]	2020	The challenge of scalability is addressed, and a framework for anomaly detection in a fog environment is proposed.	UNSW's Bot-IoT dataset	Convolutional Deep Learning (CDL)
Almiani et al. [2]	2020	An artificially fully automated IDS against cyberattacks was presented. The proposed model, including multi-layered RNN, was designed for fog computing security, end-users and IoT devices.	NSL-KDD	RNN
Li et al. [73]	2020	Uses a multi-CNN fusion method to propose a DL approach for intrusion detection. The feature data are separated into four sections based on the correlation, and the one-dimensional feature data are turned into a grayscale graph.	NSL-KDD	CNN
Li et al. [74]	2019	Proposes an IoT feature extraction and intrusion detection algorithm for intelligent cities based on a deep migration learning model that combines deep learning and intrusion detection technologies.	KDD CUP 99	Deep Migration Learning
Smys et al. [75]	2020	Based on a hybrid DL model, an IDS for IoT networks detection for various forms of attacks was developed.	UNSW NB15	RNN
Meidan et al. [76]	2018	Proposes a novel network-based anomaly detection method, using deep autoencoders to extract network behavior.	Bot-net datasets	Deep Autoencoders

Table 5. *Cont.*

Author	Yeah	Description	Dataset	DL Algorithm
Hodo et al. [77]	2016	A threat analysis using IoT is presented in this work. ANN is used to combat threats, while a multilevel perceptron, a form of ANN control, is trained on Internet packet traces, and its capability to thwart DDoS/DoS attacks is examined. This work focuses on classifying typical patterns of threats in an IoT network.	IoT Networks	RNN
Roopak et al. [78]	2019	Proposes DL models for IoT network cybersecurity.	CICIDS2017	CNN
Ullah et al. [79]	2019	Combines different strategies for detecting pirated and malware-infected software throughout the IoT network.	Google Code Jam (GCJ)	CNN
Farivar et al. [8]	2020	Presents a hybrid intelligent classic control technique for the reconstruction and compensating of cyber-attacks initiated on nonlinear cyber-physical systems (CPS) and industrial IoT systems.	Simulation	Neural Network (NN)
Saharkhizan et al. [80]	2020	Develops a technique to detect cyber threats against IoT systems with enhanced deep learning models. A set of deep RNNs was developed to detect IoT cyber-attacks via network traffic.	Modbus Network Traffic	RNN
Jahromi et al. [81]	2021	Presents the two-tier CPS detection and attribution framework for attacks in industrial control system (ICS). On the first level, the DT is designed to detect attacks in an imbalanced ICS environment, paired with a new ensemble deep representation learning model.	ICS datasets	DNN
Al-Haija and Zein-Sabatto [10]	2020	Proposes new detection and classification systems for cyber threats in IoT networks.	NSL-KDD	CNN
Thamilarasu and Chawla [82]	2019	The authors developed a smart IoT-adapted IDS for detecting malicious communication in IoT networks.	IoT network-traffic (Simulation)	DBN, DNN
Vega-barbas et al. [83]	2021	Proposes a system of IoT-focused intrusion detection and an assessment of several preprocessing strategies using traffic categorization.	UGR16, UNSW-NB15, KDD99.	Multi-layer Perceptron Neural Network (MLPNN)

4.2.3. Summary of Studies Classified Based on Model Performance

Table 6 summarizes the studies classified based on a number of predictive features and model performance. Most studies focused on the IoT environment using one of the following: ARM-based IoT applications, IoT/fog networks, Bot-IoT traffic, IIoT, healthcare IoT, power grid, smart city and IoT traffic. Conversely, performance focus determines the input of cybersecurity detection, which includes the detection of new malware samples in IoT applications/devices, effective attack detection of threats owing to the use of AI methods in IoT, and anomaly intrusion identification. Additionally, a number of predictive features, characteristics or attributes are used as a value that determines the resulting outcome of cybersecurity detection. To evaluate AI models different evaluation metrics have been used which include accuracy (ACC), precision (PRE), recall (REC), and f-measure (F1). In addition, Figure 7 shows the frequency of model performance of the studies.

Table 6. Summary of studies classified based on model performance.

Authors	Performance Focus	Number of Predictive Features	Model Performance			
			ACC (%)	PRE (%)	REC (%)	F1 (%)
Diro and Chilamkurti [7]	IoT/fog network	123	99.20	99.02	99.27	99.14
Rathore & Park [25]	IoT devices	41	86.53	-	-	86.35
Shafiq et al. [57]	BoT-IoT network	44	99.7	1.00	0.99	-
Rahman et al. [58]	IoT network	154	99.97	-	-	99.94
Roldán et al. [59]	IoT network	-	-	0.99	1	0.99
Dovom et al. [61]	IoT network	-	99.83	100	98.73	0.99
Wang et al. [62]	IoT power grid	128	93.91	0.94	0.94	0.94
Hasan et al. [63]	IoT sensors	13	99.4	0.99	0.99	0.99
Bhatia et al. [64]	IoT devices	7	90	0.99	0.99	0.99
Doshi et al. [65]	IoT traffic	5	0.99	0.99	0.99	0.99
Alrashdi et al. [67]	IoT smart city	49	99.34	0.98	0.98	0.98
Azmoodeh et al. [68]	IoT network	-	94.27	89.19	95.65	92.31
Rashid et al. [70]	IoT devises networks	78	95.45	0.95	0.95	0.95
Haddadpajouh et al. [71]	ARM-based IoT applications	681	98.18	-	-	-
G and Selvakumar [72]	Bot-IoT traffic	43	99.7	99.99	99.75	-
Almiani et al. [2]	IoT devises traffic	26	92.42	90.30	-	-
Li et al. [73]	Industrial IoT	41	86.95	90.85	86.63	88.69
Smys et al. [75]	IoT network	-	98.6	1	1	0.99
Hodo et al. [77]	IoT network	-	99.4	-	-	-
Roopak et al. [78]	IoT network	-	97.16	98.44	99.1	-
Ullah et al. [79]	IoT network	-	97.46	97.43	97.46	97.44
Saharkhizan et al. [80]	IoT network traffic	83	99.62	99.41	98.88	99.14
Jahromi et al. [81]	CPS	17	98.14	0.98	0.98	0.98
Al-Haija and Zein-Sabatto [10]	IoT network	123	99.3	99.04	99.33	99.18
Thamilarasu & Chawla [82]	IoT networks traffic	8	-	-	95	97
Vega-barbas et al. [83]	IoT network	49	0.99	0.99	0.99	-
Al Hammadi et al. [84]	IoT framework	5	0.96	0.94	0.88	0.92
Aldhaheri et al. [85]	IoT network	10	98.73	99.17	98.36	98.77%

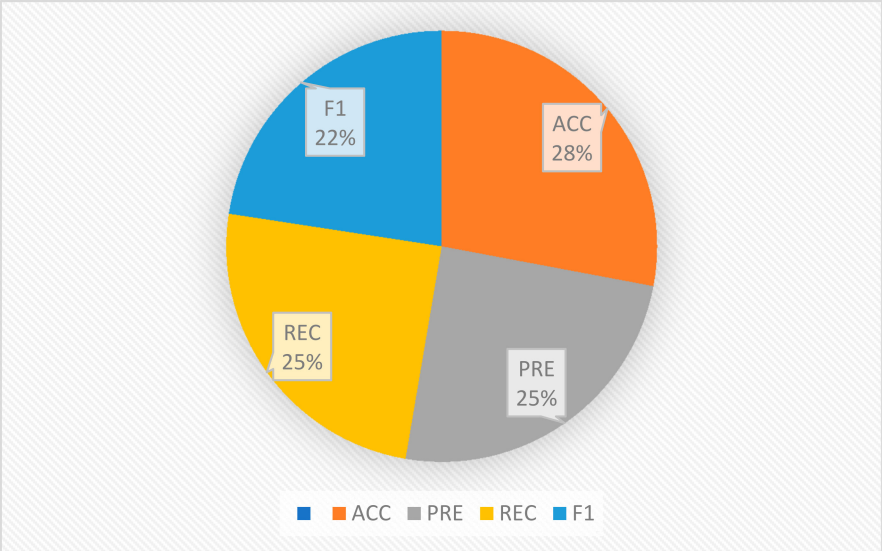

Figure 7. The frequency of model performance of the studies.

4.2.4. Summary of Studies Classified Based on IDSs and Types of Threats

Table 7 summarizes the classification of the selected studies based on IDSs, strategies, detection categories, and types of detection/attack/threat in the IoT. According to the selected studies, most researchers used hybrid, centralized, and distributed strategies with ARM-based IDS, distribution-based IDS, anomaly-based IDS, fog computing-based IDS, and specification-based IDS as detection categories. The types of detection/attack/threat include malware attacks, denial-of-service (DoS), distributed denial-of-service (DDoS), message queuing telemetry transport DoS (MQTT DoS), botnet, network, ramping, blackhole, reconnaissance, sinkhole, wormhole attacks, and network traffic categorization.

Table 7. Summary of studies classified based on IDSs and types of threats.

Authors	Strategy	Detection Category	Threat/Attack Types
Haddadpajouh et al. [71]	Hybrid	ARM-based IDS	Malware attack
Diro and Chilamkurti [7]	Centralized	Distributed based IDS	Probe, R2L, U2R, DoS
G and Selvakumar [72]	Distributed	Anomaly-based IDS	DDoS, DoS, Reconnaissance, Theft
Shafiq et al. [57]	Hybrid	Anomaly-based IDS	Malicious attack
Almiani et al. [2]	Distributed	Fog computing-based IDS	DoS, Probe, R2L, U2R
Li et al. [73]	Hybrid	Anomaly-based IDS	Dos, Probe, R2L, U2R
Rahman et al. [58]	Distributed	Anomaly-based IDS	Malicious attack
Li et al. [74]	Hybrid	Specification-based IDS	Dos, Probe, R2L, U2R
Roldán et al. [59]	Hybrid	Specification-based IDS	MQTT DoS
Li et al. [60]	Hybrid	Collaborative based IDS	False alarm reduction, Detection performance
Dovom et al. [61]	Hybrid	Specification-based IDS	Malware, Ransomware
Rathore and Park [25]	Distributed	Fog-based IDS	Dos, Probe, R2L, U2R
Wang et al. [62]	Hybrid	Specification-based IDS	Network attack
Hasan et al. [63]	Hybrid	Anomaly-based IDS	DoS
Smys et al. [75]	Hybrid	Anomaly-based IDS	Network attack
Alrashdi et al. [67]	Distributed	Anomaly-based IDS	Malicious attack
Azmoodeh et al. [68]	Hybrid	Specification-based IDS	Ransomware detection
Meidan et al. [76]	Hybrid	Anomaly-based IDS	Botnet attacks, network attack
Bhatia et al. [64]	Hybrid	Anomaly-based IDS	Denial of service attacks
Hodo et al. [77]	Distributed	Anomaly-based IDS	DDoS/DoS attacks
Doshi et al. [65]	Hybrid	Anomaly-based IDS	DDoS attacks
Roopak et al. [78]	Hybrid	Specification-based IDS	DDoS attack

Table 7. *Cont.*

Authors	Strategy	Detection Category	Threat/Attack Types
An and Liu, [66]	Distributed	Anomaly-based IDS	Ramping attack
Ullah et al. [79]	Hybrid	Specification-based IDS	Malware attack
Farivar et al. [8]	Hybrid	Specification-based IDS	Malicious attack
Saharkhizan et al. [80]	Distributed	Specification-based IDS	Network attack
Jahromi et al. [81]	Hybrid	Anomaly-based IDS	DoS, Reconnaissance
Soe et al. [69]	Distributed	Specification-based IDS	DDoS attack
Al-Haija and Zein-Sabatto [10]	Distributed	Anomaly-based IDS	Dos, Probe, R2L, U2R
Rashid et al. [70]	Hybrid	Anomaly-based IDS	DoS, DDoS, reconnaissance
Thamilarasu and Chawla [82]	Distributed	Anomaly-based IDS	DDoS, blackhole, opportunistic service, Sinkhole, wormhole Attack
Vega-barbas et al. [83]	Distributed	Anomaly-based IDS	Network traffic categorization

5. Major Findings Based on the Research Questions

5.1. RQ1: What Are the Existing Cybersecurity Attacks and Threats in the IoT Environment?

To identify the existing cybersecurity attacks, threats, and vulnerabilities in IoT (RQ1), our study confirmed the existence of DoS, DDoS, malicious, ransomware, blackhole, sinkhole, reconnaissance, and wormhole attacks (Table 7) in IoT environments. Additionally, Wang et al. [62] proposed a network attack detection model of power grid disturbances to identify cyberattacks. Rathore and Park [25] introduced fog-based attack detection considering the attack categories of the IoT ecosystem, namely DoS, probe, user-to-root (U2R), and remote-to-local (R2L) attacks. Dovom et al. [61] introduced ransomware and malware attack detection in IoT. Li et al. [60] evaluated the performance of false alarm reduction to enhance collaborative intrusion detection in IoT environments, and Azmoodeh et al. [68] proposed non-malicious applications to detect ransomware by monitoring the energy consumption patterns based on the power consumption of Android devices. Furthermore, our study explores IoT security by identifying existing features and fault identification, which are a vulnerability of IoT that leads to unreliable network and data communication. Vulnerabilities in IoT are increasing rapidly owing to the complexity of network traffic, the addition of network communication protocols, weak credentials, privacy, and insecure networks. Additionally, Diro and Chilamkurti [7] reported unauthorized access to local user accounts and a spy breaking into the system to obtain confidential information as vulnerabilities in the IoT with internet message access protocol (IMAP); these attacks can be categorized as R2L. Rashid et al. [70] added that vulnerabilities can occur through zero-day attacks by exploiting different protocols in the IoT. Therefore, when vulnerable data/information leaks are subjected to cybersecurity threats, the IoT becomes compromised by providing false results that lead to a sophisticated attack. Lastly, Table 8 illustrates the types of attacks within the IoT environment.

Table 8. List of attacks categories in IoT environment.

Attack Category	Attacks Types
Probe	mscan, portsweep, satan, nmap
U2R	httptuneel, sqlattack, loadmodule, rootkit
R2L	worm, snmpgetattack, imap, warezmaster
DoS	processtable, udpstorm, neptune, teardrop

5.2. RQ2: What Are the Common AI Methods Used to Detect Cybersecurity Attacks in the IoT?

We believe that support vector machines (SVM) and random forest (RF) are mostly used because of high accuracy detection another reason may be efficient memory. The study [58,59,61,63–66,68–70] used SVM and RF due to their classifiers effectiveness. They are widely implemented in various domains such as anomaly intrusion detection systems

in IoT environments because of their most efficient features from others ML algorithms towards identification of attacks with better performance. In addition, they are used for feature selection techniques to achieve high accuracy performance. However, they have limitations such as long CPU time from SVM and ineffective real-time predictions from RF. The studies from Alrashdi et al. [67] used the random forest method to propose a system for anomaly detection in IoT (AD-IoT), and Rahman et al. [58] used a support vector machine to address the limitations of centralized IDS for resource-constrained devices. They proposed two techniques, namely semi-distributed and distributed, which combine high-performance feature extraction and selection with potential fog-edge coordinated analytics. Furthermore, DL methods based on artificial neural networks are commonly used for cybersecurity detection (Table 5).

In addition, we find out that HaddadPajouh et al. [71] used a recurrent neural network for detecting and hunting malware in IoT. Diro and Chilamkurti [7] used the DL method for cybersecurity to enable the detection of attacks in the social IoT based on a distributed approach, and Meidan et al. [76] used deep autoencoders to propose a novel network-based anomaly detection method for detecting unusual network traffic from exploited IoT devices. Other studies combine various AI methods for cybersecurity in IoT, which serve as hybrid methods. Additionally, Smys et al. [75] used a hybrid IDS for IoT, wherein the proposed IDS detected different types of attacks based on a hybrid convolutional neural network model.

However, with the rapid development of ML and DL such as LSTM, XGBoost, CNN, NN, TCN, models provide efficient classification with high accuracy. We found that [72,74,77,79,83] used LSTM techniques with potential of RNN to hunt IoT malware and OpCodes sequence. The LSTM model is capable of learning on dependencies with input datasets. In addition, the advancements models techniques classification, prediction time series data to detect cybersecurity attacks within IoT environment. The LSTM structure has memory that stores previous time step information similar to blockchain technology. XGBoost techniques significantly improved based on boosting algorithms in cybersecurity such as to detect power grid cyber-attacks [62]. However, most studies from literature used single model technique with evaluating the model using NSL-KDD, KDD99 datasets. While at the current stage those datasets are outdated, we suggest using updated detests from real-world, real-time IoT systems. Multiple models can be combined to archive better results, performance and high detection techniques.

5.3. RQ3: What Are the Available Practices to Reduce Cybersecurity Attacks for IoT Using AI Approaches?

We found that many AI approaches have been proposed by researchers to tackle, reduce cybersecurity attacks in IoT systems. The available methods include smart intrusion detection systems, anomaly detection techniques, and intelligent architectural frameworks. An efficient DL based classification and technique has been used to detect cyber-attacks in IoT networks communications through the development of new autonomous DL classification systems using CNN [10]. AI-based data encryption enhances intermediates nodes of IoT systems [12]. In addition, AI approaches explore IoT data features extraction and provide intrusion detection systems with feature extractions for smart cities based on deep migration learning model [74]. However, the current AI techniques have limitations such as long training time due to large input datasets and high computational complexity. In addition, we suggest improving efficiency of AI models with a combination of models for better performance and high detection techniques.

6. Artificial Intelligence Roadmap

In this section, we provide an AI roadmap with brief overview of its development in detecting cybersecurity attacks within IoT systems. The methods have been categorized based on the cybersecurity threats they identify such as Probe, U2R, R2L and DoS as shown in Figure 8.

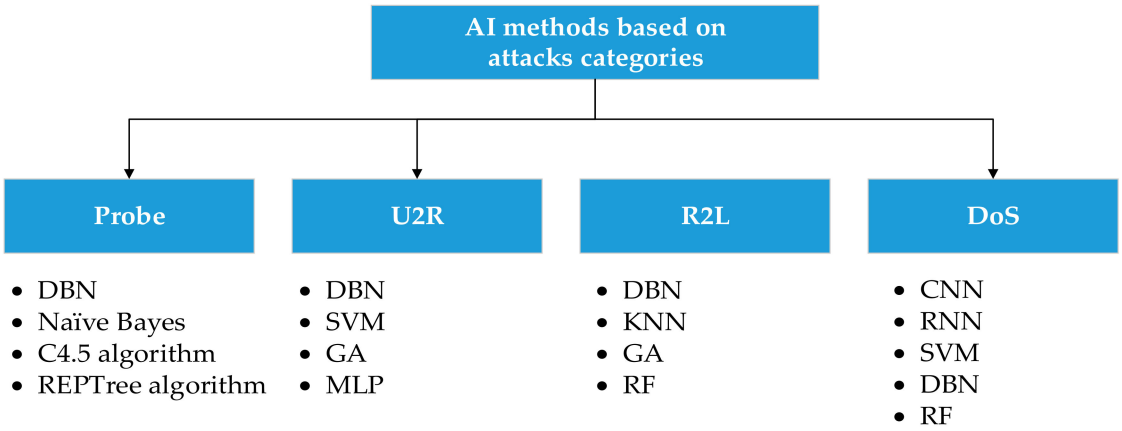

Figure 8. Illustration of artificial intelligence methods based on attacks categories.

6.1. AI for Detecting Probe Attack

Probe attacks aim to obtain data based on target external network sources such as portsweep and IPsweep. The effects of probe attacks make data vulnerable within peer networks which gives an attacker the ability to spy, access, or gather information. This attack can be detected using AI-based techniques. For example, Zhang et al. [86] proposed an IDS model based on genetic algorithm (GA) and deep belief network (DBN) to achieve a high detection rate in IoT systems. In addition, a fast intrusion detection system was proposed using hybrid AI techniques such as RF, Naïve Bayes, C4.5, REPTree algorithm to detect attacks [87].

6.2. AI for Detecting U2R Attack

User to root (U2R) attack aims to have access into systems as normal account such attacks include perl and xterm. The effects of U2R attacks include manipulating, spying or interrupting normal system behavior. In Bagaa et al. [88], a novel SVM model was proposed based on a security framework to enable mitigating different threats such as U2R in IoT systems. In addition, a GA has been proposed for generating rules to detect U2R threats [89].

6.3. AI for Detecting R2L Attack

Remote to user (R2L) attacks occur when a user sends packets to system which do not have legal access such as xclock and guest password. The effects of R2L attacks exploit system privileges. AI methods for detecting R2L attacks include Chatterjee and Hanawal [90]. In the paper, a federated learning IDS was proposed based on a probabilistic hybrid ensemble classifier (PHEC) using KNN and RF to centralize IoT security. Moreover, a GA was proposed for generating rules to detect R2L attacks [89].

6.4. AI for Detecting DoS Attack

Denial of services (DoS) attack is among the most common, due to its easy execution. It can be performed by disturbing the network traffic such as DDoS and UDP storm. The effects of DoS attacks make system resources very busy to serve networking genuine requests. An AI detection model has been proposed using various ML/DL techniques which include CNN, RNN and SVM to detect DoS attacks in IoT Botnets datasets [88,91].

7. Discussion

In this section, we discuss our study findings in terms of the research questions presented in Section 1. We summarize the major findings and explain the limitations of our systematic literature review (SLR). Finally, recommendations for future investigations are presented. Our analysis and evaluation from empirical studies revealed that several vulnerabilities and threats that can lead to attacks exist in the IoT environment. Moreover,

these attacks compromise the integrity of the IoT, which behaves abnormally during event processing owing to malicious activities. With the rapid increase in the number of IoT devices resulting from the emergence of Industry 4.0, security aspects must be prioritized. AI methods are the most promising approach for overcoming these security issues through the detection and identification of threats and attacks using smart IDSs and intelligent architectural frameworks. Moreover, the AI methods vary for different types of ML/DL in terms of event processing performance in an IoT environment.

As shown in Table 9, we indicate some selected AI models currently trending. The OIE contribute towards model extracting information from unstructured data for valuable cyber threat information when analyzing cybersecurity report [92]. In natural language processing, transformer-based models are most effective towards detecting misinformation, machine translation, text summarization on large scale with less human effort to generate fake cyber threats intelligence text description with transformed based-model [93]. XGBoost model based on gradient boosting library also among high efficient models towards decision making, XGBoost have used for security modelling to detect cyber security based on abnormalities and multi-attacks [94]. The LSTM models play a vital role among AI models for classification, prediction on time series data based on a recurrent neural network, LSTM technique have been used to introduce a deep frequency decomposition model to achieve stock prediction [95]. EBM model provides generative model from statistical physics used self-supervised learning based on EBM for equilibrium thermodynamics due to its softmax layer and mapping energies to probabilities [96]. In prediction research especially during the coronavirus disease 2019 (COVID-19). As it is been spreading within countries such as used ISI model for proposing COVID-19 prediction to estimate the infection variety for analyzing transmission laws with development trends [97]. However, the AI model has been providing a classification of misconceptions, myths and desired where the authors elaborate more on the most popular AI models with statistical methods representing characteristics models which include NN, ES, HMM, AB, and GLM [98]. Lastly, all AI models presented are effective, efficient in performance towards various applications for decisions, classification, and statistics with many more.

Table 9. List of some selected trends for artificial intelligence models.

Authors	Year	Model	Application
Sarhan and Spruit [92]	2021	Open information extraction (OIE)	Natural language processing
Ranade et al. [93]	2021	Transformer-based model	Natural language processing
Sarker [94]	2021	Extreme gradient boosting (XGBoost)	Classification, regression
Rezaei et al. [95]	2021	Long short-term memory (LSTM)	Classification, prediction, time series
Salazar [96]	2021	Energy-based model (EBM)	Statistical-mechanics
Zheng et al. [97]	2020	Improved susceptible–infected (ISI)	Natural language processing
Emmert-Streib et al. [98]	2020	Neural networks (NN)	Classification
		Expert system (ES)	Knowledge-based decisions
		Reinforcement learning (RL)	Decisions
		Adaptive boosting (AB)	Classification
		Generalized linear models (GLM)	Regression, statistical modelling

As shown in Table 10, the state-of-art are listed from previous studies with providing insight on cybersecurity attacks detection using AI techniques to detect threats in IoT environments. Notably, intrusion detections systems and anomaly-based detection are most used due to their efficient performance. While some studies applied hybrid performance to solve IoT network issues. To further improve AI performance towards predicting attacks, malware analyses and anomaly detection, current techniques need to be enhanced.

We suggest researchers focus more on combining trending AI models, development of architectural intelligence framework and increasing accuracy performance.

Table 10. List of state-of-art studies with pros and cons.

Author	Yeah	Techniques	Methodology	Pros	Cons
Shafiq et al. [57]	2020	NB, BayesNet, DT, RF	Proposed a hybrid framework to solve Bot-IoT attack traffic	- High recognition, accuracy detection. - Handling missing, error datasets.	- High model training time - High computational complexity
Li et al. [60]	2020	KNN, SVM, RF, DT	Proposed semi-supervised learning to investigate the performance of DAS-CIDS in IoT networks.	- High dimensional space - Efficient memory High recognition, accuracy detection. - Handling missing, error datasets.	- Interpretation of results needs enhancement. - High model training time - High computational complexity.
Rathore and Park [25]	2018	Fuzzy C-Means Algorithm	Proposed a fog-based attack detection framework and ELM-based in semi-supervised fuzzy C-means.	- Good classification	- Poor handling high dimensional data sets.
Wang et al. [62]	2019	KNN, SVM, DT, RF, XGBoost	Proposed ML model for attack detection of power systems using information and logs.	- High dimensional space - Efficient memory - High recognition, accuracy detection. - Handling missing, error datasets.	- Interpretation of results needs enhancement. - High model training time - High computational complexity
Hasan et al. [63]	2019	LR, SVM, DT, RF	Proposed several ML to predict attacks and anomalies on IoT systems.	- High dimensional space - Efficient memory - High recognition, accuracy detection.	- Interpretation of results needs enhancement. - High model training time - High computational complexity
Bhatia et al. [64]	2019	SVM	Proposed anomaly detection approach for network-centric based on behaviour learning.	- High dimensional space - Efficient memory	- Interpretation of results needs enhancement.
Doshi et al. [65]	2018	KNN, SVM, DT, RF	Proposed DDoS detection in IoT networks using a variety of ML techniques.	- High dimensional space - Efficient memory - High recognition, accuracy detection. - Handling missing, error datasets.	- High model training time - High computational complexity Interpretation of results needs enhancement.
Alrashdi et al. [67]	2019	RF	Proposed an anomaly detection in IoT system based on RF learning algorithms.	- Improved accuracy - Works well with categorical and continuous value	- High computational power - High training time
Azmoodeh et al. [68]	2018	KNN, SVM, RF	Proposed ransomware attack detection system based on ML by monitoring power consumption of Android devices.	- High dimensional space - Efficient memory	- Interpretation of results needs enhancement.

Table 10. *Cont.*

Author	Yeah	Techniques	Methodology	Pros	Cons
Soe et al. [69]	2020	RF	Proposed algorithm for feature selection towards lightweight detection system to detect attacks in IoT environment.	- Improved accuracy - Works well with categorical and continuous value	- High computational power - High training time
Rashid et al. [70]	2020	SVM, DT, RF, KNN	Explore anomaly detection techniques based on ML to defend IoT cybersecurity threats in smart city.	- High dimensional space - Efficient memory - High recognition, accuracy detection. - Handling missing, error datasets.	- High model training time - High computational complexity Interpretation of results needs enhancement.
Haddadpajouh et al. [71]	2018	RNN	Explore the potential of RNN in detecting malware to analyse ARM-based IoT applications.	- Enhanced robustness. - Good in time series prediction	- Detection of accuracy need enhancement. - Gradient exploding
Almiani et al. [2]	2020	RNN	Proposed fog security against cyber-attack using an artificial fully automated intrusion detection system.	- Enhanced robustness. - Good in time series prediction	- Detection of accuracy need enhancement. - Gradient exploding
Li et al. [74]	2019	DML	Proposed intrusion detection algorithms and IoT feature extraction based on deep migration learning with a combination of deep learning models.	- Real-time IDS	- Detection of accuracy need enhancement.
Smys et al. [75]	2020	RNN	Proposed intrusion detection system for IoT networks based on CNN model.	- Enhanced robustness. - Good in time series prediction	- Detection of accuracy need enhancement. - Gradient exploding
Jahromi et al. [81]	2021	DNN	Proposed two-level ensemble attack detection based on a decision tree with novel deep representation learning in IoT enabled CPSs.	- Enhanced robustness.	- Detection of accuracy need enhancement.
Vega-barbas et al. [83]	2019	Multiple-layer perceptron neural network	Proposed several techniques from traffic categorization for IoT intrusion detection system based ML neural network algorithms.	- Capable fault tolerance: - Parallel processing capability	- High computational complexity

8. Limitations of the Study

Our SLR comprehensively summarizes the empirical studies using only 80 research articles based on a search strategy by examining several databases, including SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI. Consequently, certain related studies may not be included as the search was performed considering journal papers published over five years (2016–2021). Moreover, non-English studies were excluded. In addition, some database searches are excluded such as Springer.

After a critical analysis, we determined that several proposed frameworks are weak in terms of methodology and data analysis, which leads to an outcome with low accuracy.

Additionally, each proposed system has certain problems that have not yet been solved. Although the results of certain studies are in different metric performances, we focused more on results in terms of accuracy (%) when analyzing IoT security using AI methods. In addition, it is worth mentioning that several studies did not report the predictive features of their datasets. Finally, our paper has some potential extensions and further applications but we are unable to investigate several threats which include fault injection, jamming in the IoT environment.

9. Recommendations for Future Investigations

Owing to the rapid development and increase in the use of IoT devices in various sectors, which include IIoT, medical IoT, energy IoT, and CPS, we recommend further investigation of the existing AI algorithms by introducing next-generation approaches in IoT security and privacy. Additionally, search databases other than SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI should be analyzed.

Our results reveal that different AI approaches have been proposed and implemented by researchers based on ML/DL algorithms, including hybrid methods that combine different algorithms. This implies that improving the existing intelligent architectural frameworks can aid in introducing different AI methods of ML/DL with better performance.

Our results also, verify the existence of different types of cybersecurity attacks, such as DDoS, sinkhole, wormhole, and ramping attacks, in the IoT environment. Although these attacks are categorized as DoS, probe, R2L, and U2R attacks, researchers can explore vulnerabilities beyond these categories. Moreover, the most vulnerable layer in IoT needs to be identified.

Further work also needs to be performed in improving the detection accuracy as well as concentrating on the availability of recent real-world datasets in order to detect new types of IoT threats. Finally, we anticipate our SLR results will encourage further inspiration in developing new IDS/AI models to secure the IoT environment against cybersecurity threats and attacks.

10. Conclusions

In this paper, we present a systematic review of cybersecurity detection attacks in the IoT using AI methods. Due to their rapid development in the various domains, large amounts of data are constantly being generated, which requires an increased focus on privacy and security. Attacks in IoT can be categorized into Probe, R2L, U2R, and DoS. If these attacks succeed, IoT performance can be compromised in many ways such as giving false information. While in the past, traditional methods have been used for improving IoT security, due to the rapid evolution of cyber threats. As a result of industrial 4.0, the AI approach can be considered one of the most promising methods.

We summarized, categorized, and mapped the existing literature on AI methods for the detection of cybersecurity attacks in IoT environments using formulated research questions. The survey was conducted using the PRISMA method, wherein eighty studies from 2016 to 2021 were carefully selected and evaluated. However, the SLR validates that AI approaches are a promising method for providing security and privacy in IoT environments.

Author Contributions: Conceptualization, M.A. and Y.B.; funding acquisition, H.A. and A.A; methodology, M.A. and Y.B.; supervision, H.A., N.A., L.F.C. and S.J.A.; writing—original draft, M.A. and Y.B.; writing—review and editing, Y.B., H.A., A.A., N.A., L.F.C. and S.J.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research was funded by Researchers Supporting Project Number (RSP-2021/309), King Saud University, Riyadh, Saudi Arabia and Yayasan Universiti Teknologi Petronas under the research grant (015LC0-286).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: This research was supported by a Researchers Supporting Project Number (RSP-2021/309), King Saud University, Riyadh, Saudi Arabia. The authors wish to acknowledge Yayasan Universiti Teknologi Petronas for supporting this work through the research grant (015LC0-286).

Conflicts of Interest: The authors declare that there are no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AB	Adaptive Boosting
ACC	Accuracy
AI	Artificial Intelligence
AIS	Artificial Immune Systems
ANN	Artificial Neural Network
CPS	Cyber-physical Systems
CNN	Convolutional Neural Network
DA	Deep Autoencoders
DBN	Deep Belief Networks
DL	Deep Learning
DNN	Deep Neural Network
DWH	Data Warehouse
DT	Decision Tree
DoS	Denial-of-service
DDoS	Distributed Denial-of-service
ELM	Extreme Learning Machine
ES	Expert System
FPT	Fuzzy Pattern Tree
F1	F-measure
GLM	Generalized linear models
GA	Genetic Algorithm
HMM	Hidden Markov Models
IoT	Internet of Things
IIoT	Industrial IoT
ICS	Industrial Control System
IDS	Intrusion Detection Systems
ISI	Improved Susceptible-Infected
k-NN	k-nearest Neighbors Algorithm
LSTM	Long short-term Memory
LR	Logistic Regression
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NB	Naïve Bayes
NN	Neural Networks
OIE	Open Information Extraction
PRE	Precision
PHEC	Probabilistic Hybrid Ensemble Classifier
RNN	Recurrent Neural Networks
REC	Recall
RF	Random Forest
RL	Reinforcement Learning
R2L	Remote to LOCAL
SDN	Software-defined Networking
SLR	Systematic Literature Review
SVM	Support Vector Machine
SVR	support Vector Regression
U2R	User to Root
XGBoost	Extreme Gradient Boosting

References

1. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the Next-Generation Networks and Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3515–3520. [CrossRef]
2. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* **2020**, *101*, 102031. [CrossRef]
3. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. *Futur. Gener. Comput. Syst.* **2022**, *127*, 286–296. [CrossRef]
4. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. *Sustain. Cities Soc.* **2021**, *75*, 103311. [CrossRef] [PubMed]
5. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4166–4176. [CrossRef]
6. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and multidirectional data aggregation for edge computing-enhanced IoT. *J. Syst. Archit.* **2020**, *106*, 101713. [CrossRef]
7. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]
8. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2716–2725. [CrossRef]
9. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
10. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics* **2020**, *9*, 2152. [CrossRef]
11. Zhang, T.; Zhao, Y.; Jia, W.; Chen, M.Y. Collaborative algorithms that combine AI with IoT towards monitoring and control system. *Futur. Gener. Comput. Syst.* **2021**, *125*, 677–686. [CrossRef]
12. Li, B.; Feng, Y.; Xiong, Z.; Yang, W.; Liu, G. Research on AI security enhanced encryption algorithm of autonomous IoT systems. *Inf. Sci.* **2021**, *575*, 379–398. [CrossRef]
13. Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet Things* **2021**, *15*, 100420. [CrossRef]
14. Obaidat, M.A.; Obeidat, S.; Holst, J.; Hayajneh, A.A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
15. Li, J.; Kuang, X.; Lin, S.; Ma, X.; Tang, Y. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. *Inf. Sci.* **2020**, *526*, 166–179. [CrossRef]
16. Sarica, A.K.; Angin, P. Explainable security in SDN-based IoT networks. *Sensors* **2020**, *20*, 7326. [CrossRef] [PubMed]
17. Aleem, S.; Capretz, L.F.; Ahmed, F. Security Issues in Data Warehouse. *arXiv* **2015**, arXiv:1507.05644.
18. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.* **2019**, *30*, 1111–1123. [CrossRef]
19. Patil, R.; Dudeja, H.; Modi, C. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. *Int. J. Inf. Secur.* **2020**, *19*, 147–162. [CrossRef]
20. Dang, T.K.; Pham, C.D.M.; Nguyen, T.L.P. A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities. *Sustain. Cities Soc.* **2020**, *56*, 102097. [CrossRef]
21. Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustain. Cities Soc.* **2021**, *72*, 102994. [CrossRef]
22. Atul, D.J.; Kamalraj, R.; Ramesh, G.; Sakthidasan Sankaran, K.; Sharma, S.; Khasim, S. A machine learning based IoT for providing an intrusion detection system for security. *Microprocess. Microsyst.* **2021**, *82*, 103741. [CrossRef]
23. Ghosh, A.; Chakraborty, D.; Law, A. Artificial intelligence in Internet of things. *CAAI Trans. Intell. Technol.* **2018**, *3*, 208–218. [CrossRef]
24. Bland, J.A.; Petty, M.D.; Whitaker, T.S.; Maxwell, K.P.; Cantrell, W.A. Machine Learning Cyberattack and Defense Strategies. *Comput. Secur.* **2020**, *92*, 101738. [CrossRef]
25. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. *Appl. Soft Comput. J.* **2018**, *72*, 79–89. [CrossRef]
26. Kasongo, S.M.; Sun, Y. A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Comput. Secur.* **2020**, *92*, 101752. [CrossRef]
27. Chmiel, M.; Korona, M.; Kozioł, F.; Szczypiorski, K.; Rawski, M. Discussion on iot security recommendations against the state-of-the-art solutions. *Electronics* **2021**, *10*, 1814. [CrossRef]
28. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Barnawi, A.; Alzahrani, B.A. Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. *J. Netw. Comput. Appl.* **2020**, *157*, 102537. [CrossRef]
29. Quintal, K.; Malton, A.; Walenstein, A. Biometric Signatures for Continuous Authentication. *Digit. Object Identifier* **2019**, *23*, 18–28. [CrossRef]

30. Lu, X.; Pan, Z.; Xian, H. An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Comput. Secur.* **2020**, *92*, 101686. [CrossRef]
31. Kim, S.; Hwang, C.; Lee, T. Anomaly based unknown intrusion detection in endpoint environments. *Electronics* **2020**, *9*, 1022. [CrossRef]
32. Choo, K.K.R.; Yan, Z.; Meng, W. Editorial: Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges, and Opportunities. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4119–4121. [CrossRef]
33. Almusaylim, Z.A.; Alhumam, A.; Jhanjhi, N.Z. Proposing a Secure RPL based Internet of Things Routing Protocol: A Review. *Ad Hoc Netw.* **2020**, *101*, 102096. [CrossRef]
34. Viejo, A.; Sánchez, D. Secure monitoring in IoT-based services via fog orchestration. *Futur. Gener. Comput. Syst.* **2020**, *107*, 443–457. [CrossRef]
35. Singh, R.; Kumar, H.; Singla, R.K. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Syst. Appl.* **2015**, *42*, 8609–8624. [CrossRef]
36. Sáez, J.A.; Krawczyk, B.; Woźniak, M. Analyzing the oversampling of different classes and types of examples in multi-class imbalanced datasets. *Pattern Recognit.* **2016**, *57*, 164–178. [CrossRef]
37. Ahmad, Z.; Khan, A.S.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J.P.C. Anomaly detection using deep neural network for iot architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
38. Ali, S.S.; Choi, B.J. State-of-the-art artificial intelligence techniques for distributed smart grids: A review. *Electronics* **2020**, *9*, 1030. [CrossRef]
39. Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for security of Internet of Things (IoT): A survey. *J. Netw. Comput. Appl.* **2020**, *161*, 102630. [CrossRef]
40. Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Appl. Sci.* **2021**, *11*, 8383. [CrossRef]
41. Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity model based on hardening for secure internet of things implementation. *Appl. Sci.* **2021**, *11*, 3260. [CrossRef]
42. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [CrossRef]
43. Mahbub, M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *J. Netw. Comput. Appl.* **2020**, *168*, 102761. [CrossRef]
44. Dilek, S.; Cakır, H.; Aydın, M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *Int. J. Artif. Intell. Appl.* **2015**, *6*, 21–39. [CrossRef]
45. Greensmith, J. Securing the internet of things with responsive artificial immune systems. In Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation, Madrid, Spain, 11–15 July 2015; pp. 113–120. [CrossRef]
46. Morel, B. Artificial intelligence and key to the future of cybersecurity. In Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, Chicago, IL, USA, 21 October 2011; pp. 93–97. [CrossRef]
47. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
48. Sharma, R.; Kamble, S.S.; Gunasekaran, A.; Kumar, V.; Kumar, A. A systematic literature review on machine learning applications for sustainable agriculture supply chain performance. *Comput. Oper. Res.* **2020**, *119*, 104926. [CrossRef]
49. Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Ali, A.; Nasser, M.; Abdo, S. *Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey BT—Innovative Systems for Intelligent Health Informatics*; Saeed, F., Mohammed, F., Al-Nahari, A., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 659–675.
50. Haji, S.H.; Ameen, S.Y. Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review. *Asian J. Res. Comput. Sci.* **2021**, *9*, 30–46. [CrossRef]
51. Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. *Comput. Sci. Rev.* **2021**, *40*, 100389. [CrossRef]
52. Istiaque Ahmed, K.; Tahir, M.; Hadi Habaebi, M.; Lun Lau, S.; Ahad, A. Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction. *Sensors* **2021**, *21*, 5122. [CrossRef]
53. Rjab, A.B.; Mellouli, S. Smart Cities in the Era of Artificial Intelligence and Internet of Things: Promises and Challenges. *Public Adm. Inf. Technol.* **2021**, *37*, 259–288. [CrossRef]
54. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 163–186. [CrossRef]
55. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; Altman, D.; Antes, G.; Atkins, D.; Barbour, V.; Barrowman, N.; Berlin, J.A.; et al. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med.* **2009**, *6*, e1000097. [CrossRef]
56. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Elsevier: Amsterdam, The Netherlands, 2007.
57. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Futur. Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]

58. Rahman, M.A.; Asyhari, A.T.; Leong, L.S.; Satrya, G.B.; Hai Tao, M.; Zolkipli, M.F. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102324. [CrossRef]
59. Roldán, J.; Boubeta-Puig, J.; Luis Martínez, J.; Ortiz, G. Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. *Expert Syst. Appl.* **2020**, *149*, 113251. [CrossRef]
60. Li, W.; Meng, W.; Au, M.H. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. *J. Netw. Comput. Appl.* **2020**, *161*, 102631. [CrossRef]
61. Dovom, E.M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D.E.; Parizi, R.M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *J. Syst. Archit.* **2019**, *97*, 1–7. [CrossRef]
62. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Appl.* **2019**, *46*, 42–52. [CrossRef]
63. Hasan, M.; Islam, M.M.; Zarif, M.I.I.; Hashem, M.M.A. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet Things* **2019**, *7*, 100059. [CrossRef]
64. Bhatia, R.; Benno, S.; Esteban, J.; Lakshman, T.V.; Grogan, J. Unsupervised machine learning for network-centric anomaly detection in IoT. In Proceedings of the 3rd Acm Conext Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks, Orlando, FL, USA, 9 December 2019; pp. 42–48. [CrossRef]
65. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for consumer internet of things devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35. [CrossRef]
66. An, Y.; Liu, D. Multivariate Gaussian-Based False Data Detection against Cyber-Attacks. *IEEE Access* **2019**, *7*, 119804–119812. [CrossRef]
67. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310. [CrossRef]
68. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1141–1152. [CrossRef]
69. Soe, Y.N.; Feng, Y.; Santosa, P.I.; Hartanto, R.; Sakurai, K. Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features. *Electronics* **2020**, *9*, 144. [CrossRef]
70. Rashid, M.M.; Kamruzzaman, J.; Hassan, M.M.; Imam, T.; Gordon, S. Cyberattacks detection in iot-based smart city applications using machine learning techniques. *Int. J. Environ. Res. Public Health* **2020**, *17*, 9347. [CrossRef] [PubMed]
71. HaddadPajouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.K.R. A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Futur. Gener. Comput. Syst.* **2018**, *85*, 88–96. [CrossRef]
72. NG, B.A.; Selvakumar, S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. *Futur. Gener. Comput. Syst.* **2020**, *113*, 255–265. [CrossRef]
73. Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.; Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Meas. J. Int. Meas. Confed.* **2020**, *154*, 107450. [CrossRef]
74. Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *Int. J. Inf. Manag.* **2019**, *49*, 533–545. [CrossRef]
75. Smys, S.; Basar, A. Haoxiang Wang Hybrid Intrusion Detection System for Internet of Things (IoT). *J. ISMAC* **2020**, *2*, 190–199. [CrossRef]
76. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
77. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia, 11–13 May 2016; pp. 1–6. [CrossRef]
78. Roopak, M.; Yun Tian, G.; Chambers, J. Deep learning models for cyber security in IoT networks. In Proceedings of the IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 452–457. [CrossRef]
79. Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber security threats detection in internet of things using deep learning approach. *IEEE Access* **2019**, *7*, 124379–124389. [CrossRef]
80. Saharkhizan, M.; Azmoodeh, A.; Dehghantanha, A.; Choo, K.K.R.; Parizi, R.M. An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. *IEEE Internet Things J.* **2020**, *7*, 8852–8859. [CrossRef]
81. Jahromi, A.N.; Karimipour, H.; Dehghantanha, A.; Choo, K.K.R. Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems. *IEEE Internet Things J.* **2021**, *8*, 13712–13722. [CrossRef]
82. Thamilarasu, G.; Chawla, S. Towards deep-learning-driven intrusion detection for the internet of things. *Sensors* **2019**, *19*, 1977. [CrossRef] [PubMed]
83. Vega-barbas, M.; Rivera, D.; Rodrigo, M.S. An IoT-Focused Intrusion Detection System Approach Based on. *Sensors* **2021**, *21*, 656.
84. Al Hammadi, A.Y.; Yeun, C.Y.; Damiani, E.; Yoo, P.D.; Hu, J.; Yeun, H.K.; Yim, M.S. Explainable artificial intelligence to evaluate industrial internal security using EEG signals in IoT framework. *Ad Hoc Networks* **2021**, *123*, 102641. [CrossRef]
85. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Alzahrani, B.; Al-Barakati, A. DeepDCA: Novel network-based detection of iot attacks using artificial immune system. *Appl. Sci.* **2020**, *10*, 1909. [CrossRef]

86. Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. *IEEE Access* **2019**, *7*, 31711–31722. [CrossRef]
87. Ait Tchakoucht, T.; Ezziyyani, M. Building a fast intrusion detection system for high-speed-networks: Probe and dos attacks detection. *Procedia Comput. Sci.* **2018**, *127*, 521–530. [CrossRef]
88. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. *IEEE Access* **2020**, *8*, 114066–114077. [CrossRef]
89. Paliwal, S.; Gupta, R. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm. *Int. J. Comput. Appl.* **2012**, *60*, 57–62.
90. Chatterjee, S.; Hanawal, M.K. Federated Learning for Intrusion Detection in IoT Security: A Hybrid Ensemble Approach. *arXiv* **2021**, arXiv:2106.15349.
91. Kim, J.; Shim, M.; Hong, S.; Shin, Y.; Choi, E. Intelligent detection of iot botnets using machine learning and deep learning. *Appl. Sci.* **2020**, *10*, 7009. [CrossRef]
92. Sarhan, I.; Spruit, M. Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph. *Knowl.-Based Syst.* **2021**, *233*, 107524. [CrossRef]
93. Ranade, P.; Piplai, A.; Mittal, S.; Joshi, A.; Finin, T. Generating Fake Cyber Threat Intelligence Using Transformer-Based Models. In Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN), Baltimore Country, BC, USA, 18 June 2021; pp. 1–9.
94. Sarker, I.H. CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet Things* **2021**, *14*, 100393. [CrossRef]
95. Rezaei, H.; Faaljou, H.; Mansourfar, G. Intelligent Asset Allocation using Predictions of Deep Frequency Decomposition. *Expert Syst. Appl.* **2021**, *186*, 115715. [CrossRef]
96. Salazar, D.S.P. Nonequilibrium thermodynamics of self-supervised learning. *Phys. Lett. Sect. A Gen. At. Solid State Phys.* **2021**, *419*, 127756. [CrossRef]
97. Zheng, N.; Du, S.; Wang, J.; Zhang, H.; Cui, W.; Kang, Z.; Yang, T.; Lou, B.; Chi, Y.; Long, H.; et al. Predicting COVID-19 in China Using Hybrid AI Model. *IEEE Trans. Cybern.* **2020**, *50*, 2891–2904. [CrossRef]
98. Emmert-Streib, F.; Yli-Harja, O.; Dehmer, M. Artificial Intelligence: A Clarification of Misconceptions, Myths and Desired Status. *Front. Artif. Intell.* **2020**, *3*, 524339. [CrossRef] [PubMed]