






Review

Learning-Based Methods for Cyber Attacks Detection in IoT Systems: Methods, Analysis, and Future Prospects

Usman Inayat ¹, Muhammad Fahad Zia ^{2,*}, Sajid Mahmood ¹, Haris M. Khalid ³
and Mohamed Benbouzid ^{4,5}

- ¹ Department of Informatics & Systems, School of Systems & Technology, University of Management and Technology, Lahore 54770, Pakistan; usman.inayat@umt.edu.pk (U.I.); sajid.mahmood@umt.edu.pk (S.M.)
- ² Department of Electrical Engineering, National University of Computer and Emerging Sciences, Lahore 54000, Pakistan
- ³ Department of Electrical and Electronics Engineering, Higher Colleges of Technology, Sharjah 7947, United Arab Emirates; harism.khalid@ieee.org
- ⁴ Institut de Recherche Dupuy de Lôme (UMR CNRS 6027 IRL), University of Brest, 29238 Brest, France; mohamed.benbouzid@univ-brest.fr
- ⁵ Logistics Engineering College, Shanghai Maritime University, Shanghai 201306, China
- * Correspondence: fahad.zia@nu.edu.pk

Abstract: Internet of Things (IoT) is a developing technology that provides the simplicity and benefits of exchanging data with other devices using the cloud or wireless networks. However, the changes and developments in the IoT environment are making IoT systems susceptible to cyber attacks which could possibly lead to malicious intrusions. The impacts of these intrusions could lead to physical and economical damages. This article primarily focuses on the IoT system/framework, the IoT, learning-based methods, and the difficulties faced by the IoT devices or systems after the occurrence of an attack. Learning-based methods are reviewed using different types of cyber attacks, such as denial-of-service (DoS), distributed denial-of-service (DDoS), probing, user-to-root (U2R), remote-to-local (R2L), botnet attack, spoofing, and man-in-the-middle (MITM) attacks. For learning-based methods, both machine and deep learning methods are presented and analyzed in relation to the detection of cyber attacks in IoT systems. A comprehensive list of publications to date in the literature is integrated to present a complete picture of various developments in this area. Finally, future research directions are also provided in the paper.

Keywords: cyber attacks; cyber-physical systems; deep learning; denial-of-service (DoS); detection methods; Internet of Things (IoT); machine learning; man-in-the-middle; security



Citation: Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid H.M.; Benbouzid, M. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: Methods, Analysis, and Future Prospects. *Electronics* **2022**, *11*, 1502. <https://doi.org/10.3390/electronics11091502>

Academic Editor: Taeshik Shon

Received: 30 March 2022

Accepted: 3 May 2022

Published: 7 May 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

1.1. Digitalization and IoT

The world is currently moving towards the digitization of devices and systems. Almost all systems are running their operations with the help of the Internet. However, the Internet alone is not enough for the current digital revolution of new technologies that are being developed and deployed. Nowadays, Internet of things (IoT) technology is needed in applications, devices, sensors, tools, and software to ensure better operation with precision. With the development of IoT, life is becoming easy and comfortable for human beings, industries, and governments. Devices, gadgets, sensors, and machines are becoming more intelligent; and manual involvement has been considerably reduced through the development of IoT technology [1]. IoT is needed for smart devices such as smart energy meters, smart mobiles, smart security systems, fire alarms, physical sensors in medical, industrial, and energy applications [2–7].

1.2. IoT—An Internet-Connected Framework and the Scope of This Work

IoT is defined as “a framework/system of Internet-connected, interrelated devices or objects which collect and transmit the data over the wireless network without the help of human interaction” [8]. IoT platforms enable better, cheaper, and faster IT solutions. The general architecture of an IoT system is presented in Figure 1. The important components for IoT working are: (1) network and device connectivity, (2) interaction of devices, (3) analysis, (4) devices and network management, (5) security, and (6) data storage. When these devices need to communicate and send data, they use IoT protocols and standards. IoT protocols and standards are mainly divided into two parts: (1) data protocols (MQTT, CoAP, AMQP, DDS, HTTP, and WebSocket), and (2) network protocols (WiFi, Bluetooth, ZigBee, LoRaWan, and Z-Wave). In terms of securing data or devices from malicious attacks, security protocols are needed, such as Wireless Hart, LoRaWan, LPWAN IEEE 802.15.4, DTLS, and AMQP, which form the scope of this work.

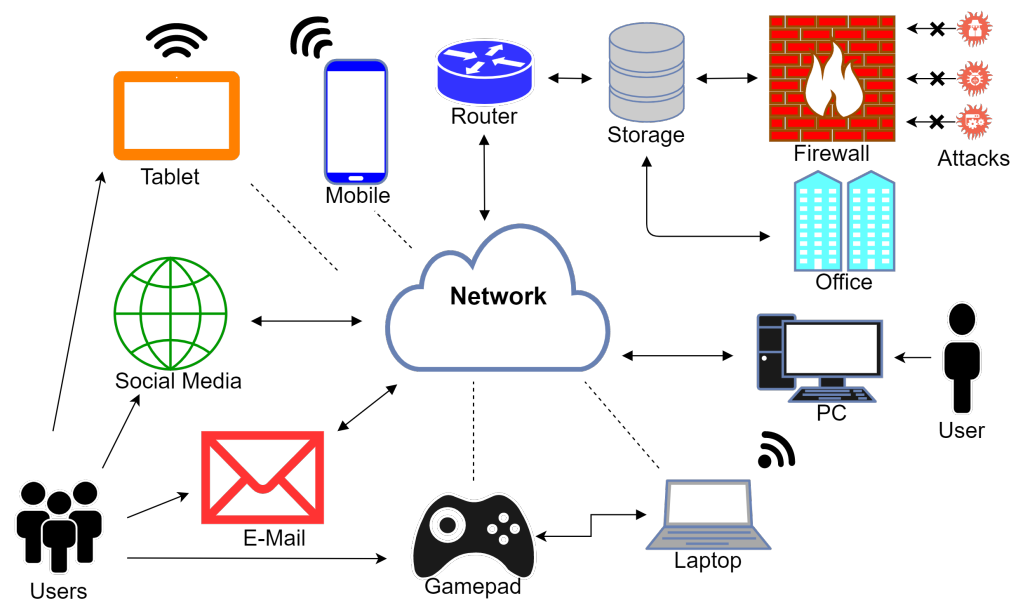


Figure 1. General representation of an IoT system.

1.3. IoT Security and Datasets

IoT security is the term used for protecting network-based or Internet-connected things. Though the idea of IoT was proposed almost two decades ago, the core terminology of IoT has been in the development phase for many years [9]. The main purpose of IoT is to connect nodes, smart cities, systems, frameworks, and sensors through the Internet for communication, data sharing, and control. IoT is designed to optimize our daily lives and the modern world to run efficiently. IoT is permeating our daily lives. Everything is connected to the Internet, such as smart sensors, fitness mobile applications, thermostats, PV systems, air conditioners, and cooking appliances [10,11]. This rapid development in IoT technology is making it harder to secure and protect IoT data from attackers, hackers, unauthorized users, and malicious traffic [12–14]. Therefore, multiple defense mechanisms and strategies are being developed and implemented in IoT systems and frameworks to protect information. Different datasets have been used in the literature to develop detection methods for malicious attacks in IoT systems. The widely used datasets are summarized in Table 1.

Table 1. Datasets used for detection of malicious attacks in IoT systems.

Datasets	Description
NSL-KDD	This dataset is used to compare different intrusion detection methods. It is also recommended to resolve KDD'99 problems. It contains nearly 4,900,000 single connection vectors. Every single vector contains 41 features and it is labeled as an attack (one specific type) or normal. Attacks are included in this dataset are DoS, R2L, U2R, and probe.
Kyoto 2006+	This dataset is constructed on real three-year network traffic data. Dataset is labeled as normal, known, and unknown attacks. It contains 14 numerical features from KDD Cup' 99 and 10 other features.
DS2OS	It is an IoT middleware that includes the service and data of smart space. It contains a set of 4,77,426 data with 14 different features which are classified into five attack classes: (1) normal, (2) DDoS, (3) MITM, (4) Scan wrong setup, (5) data type probing.
UNSW-NB15	This dataset is used for a network intrusion detection system with nine different attacks, which are: (1) backdoors, (2) worms, (3) DoS, (4) fuzzers, (5) analysis, (6) shellcode, (7) reconnaissance, (8) generic, and (9) exploit.
KDD-Cup 1999	It is used to audit the data which includes several intrusion simulations. This dataset contains up to 5,000,000 records. Each record contains 41 features which are categorized into 4 attacks of: (1) DoS, (2) R2L, (3) U2R, (4) probe.
NN-BaIoT	DDoS attack and two types of botnets. The botnets are Bashlite and Mirai, which are included in this dataset.
Urban Sound 8k	It is an audio dataset that contains 8732 labeled urban sounds, such as: (1) air-conditioner, (2) siren, (3) street music, (4) idling, (5) car-horn, (6) dog-bark, (7) children-playing, (8) drilling, (9) jackhammer, and (10) gun-shots.
CSIC 2010 HTTP	This dataset contains thousands of web requests which are generated automatically. This dataset is labeled as anomalous (25,000) and normal (36,000) requests and they contain the attacks of: (1) buffer overflow, (2) CRLF injection, (3) server-side, (4) XSS, (5) parameter tampering, (6) files disclosure, (7) SQL injection, and (8) information gathering.
ISOT	This dataset is a combination of commonly existing malicious and non-malicious datasets. It contains a variety of trace data of the network spanning from emails and web to streaming and backup media. The attacks include in this dataset are of two types of botnets: (1) Zeus, and (2) Waledac.
ADFA-LD	This dataset is based on cyber security for the evaluation of data mining-based IDS and machine learning. This dataset contains the Linux OS records. Type of attacks includes in this dataset are: (1) meterpreter, (2) Webshell, (3) hydra-SHH, (4) java-meterpreter, (5) hydra-FTP, and (6) Adduser.
IoTID20	This dataset was proposed for IDSs. It is the recent dataset used to simulate network attacks coming from two smart devices. The threats that occur in this dataset are (DoS, Mirai, scan, MITM, and normal). It contains 83 features of the network and 3 other features with 625,783 records.
UNSW's Bot-IoT	This dataset provides a combination of the botnet and normal traffic. The source files for this dataset are available in different formats of CSV, original pcap, and generated argus files. The extracted flow traffic in CSV format is 16.7 GB and captured pcap files are 69.3GB in size. The dataset includes several types of attacks like: (1) keylogging, (2) service and OS scan, (3) DoS, (4) DDoS, and (5) data exfiltration.

1.4. IoT Security and Cloud Services

To provide better IoT security, several machine learning methods have been implemented [15,16]. Moreover, cloud services are also utilized for better, more secure, low-cost, and efficient connectivity. In [17], the cipher text-policy attribute-based mechanism for keyword searching and data sharing (CPAB-KSDS) method was developed to encrypt cloud data when the cloud service provider (CSP) is searching and sharing the data with the end-user. Another advantage of this model is that it does not need public key generation (PKG) to re-encrypt the key every time. In [18], the authors introduced a scheme to check the fairness and verification of current data while handling encrypted outsourced data. The verification and fairness attribute-based proxy re-encryption (VF-ABPRE) scheme was implemented to check if the data sent by the server were correct or if there was a mali-

cious allegation in the data. For better security, the authors used verification and fairness cipher text-policy attribute-based proxy re-encryption (VF-CP-ABPRE) to secure the data. The message-lock encryption technique is used to prevent common users from seeing the plain text.

In order for the server to revoke some client's access, reference [19] presented the scheme revocable attribute-based encryption-data integrity (RABE-DI) to revoke client access even to authorized users. This model was presented to ensure the integrity of a cloud service after revocation is executed. Algorithms such as Revoke and Decre were used for more enhanced output. In [20], the authors used revocable identity-based broadcast proxy re-encryption (RIB-BPRE) so that a user could send simple data to multiple groups with a key mechanism. A key mechanism is used to achieve correct revocable notion in the proposed method. The key mechanism is needed due to the vast variety of information and the massive amount of data in cloud computing.

1.5. Defense Strategies and the Motivation for This Work

In general, the security issues faced by IoT devices are malware, weak password protection, exploitation, skill gaps, poor device management, insecure protocols, data leakage, firewall, secure booting, intrusion deception threat (IDT), authentication, and encryption [21–23]. Different methods have been utilized as defense strategies, such as (1) distributed deep learning (DDL) [24], (2) adversarial deep learning (ADL) [25], (3) the bidirectional short term memory based recurrent neural network (BLSTM-RNN) [26], (4) the artificial neural network (ANN) [27], (5) the deep neural network (DNN) [28], (6) existing network intrusion detection system (NIDS) implementation tools [29], (7) tensor DNN [30], (8) adversarial machine learning and other traditional methods (such as Petri Net) [25], (9) cloud-based distributed deep learning frameworks—(a) distributed convolution neural networks and (b) cloud based temporal long-short term memory [31]—(10) the uniform intrusion detection method [32], (11) the deep-learning-based intrusion detection system method with the combination of spider monkey optimization and a stacked-deep polynomial network [33], (12) the baptized BotIDS-based convolutional neural network [34], (13) CorrAUC [35], (14) K-nearest neighbors (KNN) and LSVM [36], (15) random forest (RF) [36–38], (16) neural networks [36,38], (17) decision trees (DTs) [36,37], and (18) supervised, unsupervised, semi-supervised, and reinforcement techniques [39,40]. However, these defense strategies do not express the deployment of semi-supervised and advanced deep learning methods, which formed the main motivation for this paper.

1.6. Preceding Affined Review Papers

The herein presented review mostly covers only the security issues, malicious attacks, and their detection mechanisms in IoT systems. The review and survey papers existing in the literature are also summarized in Table 2. The article in [41] talks about deep learning methods in cyber security. Various methods, such as deep auto-encoders, restricted Boltzmann machines, RNN, generative adversarial networks, DBN, and CNN, are described. The idea is to detect malicious botnet attacks, such as malware, spam, insider threats, false data injection, and malicious domain names. In this study, the KDD-99 dataset was used. Reference [42] is a survey of machine and deep learning methods for IoT security. Both machine and deep learning methods have been discussed to detect malicious attacks in ML/DL layers (application, network, and perception) by using multiple datasets to achieve higher security. Machine-learning-based solutions for security of IoT are described in [43]. Various machine learning methods have been discussed to identify and detect attacks and abnormal behaviors in an IoT framework. Reference [44] is a survey of IoT security. Confidentiality, integrity, and availability issues are discussed using artificial intelligence methods in an IoT environment. Deep learning and big data technologies for IoT security are discussed in [45]. This paper studies deep learning and big data technology models to provide a secure IoT environment by detecting attacks.

This article is different from the aforementioned review papers because semi-supervised machine learning methods and advanced deep learning methods are also included for the detection of cyber attacks in IoT systems and devices in this paper. Moreover, classification methods and different datasets used for cyber attack detection are also presented.

Table 2. Summary of review papers on detection of IoT cyber attacks.

Ref.	Description and Contribution
[41]	Different deep learning methods (deep auto-encoders, restricted Boltzmann machines, RNN, generative adversarial networks, DBN, and CNN) are described that detect malicious botnet attacks like malware, spam, insider threats, false data injection, and malicious domain name among others. KDD-99 dataset has been used.
[42]	Both machine and deep learning methods (DT, SVM, KNN, RF, AR, K-means, EL, PCA, CNN, RNN, AE, RBMs, DBMs, GAN, and EDLNs) have been discussed to detect malicious attacks in ML/DL layers (application, network, and perception) by using multiple datasets for achieving higher security.
[43]	Different machine learning methods (Clustering, DT, SVM, KNN, RF, NB, AR, NN, K-means, EL, RL, and PCA) have been discussed to identify and detect attacks and abnormal behaviors in an IoT framework.
[44]	Confidentiality, Integrity, and Availability issues are discussed using artificial intelligence methods in an IoT environment.
[45]	This article study deep learning and big data technologies model (RNN, DNN, DBM, MLP, ELM, ANN, AE, DRBM, CC4 neural network, Apache Spark, Apache Hadoop, and Apache Storm) to provide a secure IoT environment by detecting attacks (Botnet, DNS, and Malware).

1.7. The Necessity for an Up-to-Date Review

Through the previous reviews of the latest selected research findings, it has been shown that there are various IoT challenges and important IoT issues, structures, and key application areas to be explored. The rapid growth and widespread adoption of IoT devices makes IoT security issues more complex, which increases the need for developing network-based security solutions. While current systems are doing well at identifying cyber attacks, it is still a challenge to find all of them. As network attacks increase, and with the increase in the amount of information available on networks, faster and more efficient ways to detect attacks are needed, and there is no doubt that there is a wide range of ongoing ways to improve network security. One important IoT issue that needs attention and more research is security and privacy. The detection of cyber security attacks using AI on IoT has greatly improved. Due to this, it is essential and necessary to provide a detailed analysis by studying the previous research. Our goal was to recognize the ML and DL methods that are most effective for detecting threats and attacks on IoT systems and to explore existing methods of mitigating those attacks using effective strategies. A couple of studies have focused on the traditional methods, and others focused on strategies of deep learning for the security of IoT. In our research, we tested both ML and DL methods for IoT security and considered future directions.

The main contributions of this paper are to explore and identify the development of semi-supervised machine learning and advanced deep learning methods for the detection of cyber attacks in IoT systems and devices. We also aim to bridge the gap between feature selection methods and various datasets utilized for cyber attack detection in IoT systems and devices.

1.8. Brief Description of the Review Methodology

The literature review was conducted using a variety of data sources based on a search strategy designed to identify relevant subjects. To date, systematic computer searches have been completed using various sources of information, namely, ACM, SCOPUS, IEEE Xplore, Science Direct, MDPI, and Web of Science.

The primary selection was made with respect to several characteristics, as shown in Figure 2. The search focused on the mapping of existing literature on Internet security, machine learning, and deep learning security in the discipline of computer science. The search covered the years 2016 to 2022 and included papers from journals published in English only; we only used a few review papers. All articles published before 2016 were been included. Additionally, searches were not limited to a specific region or country and were performed at a global level.

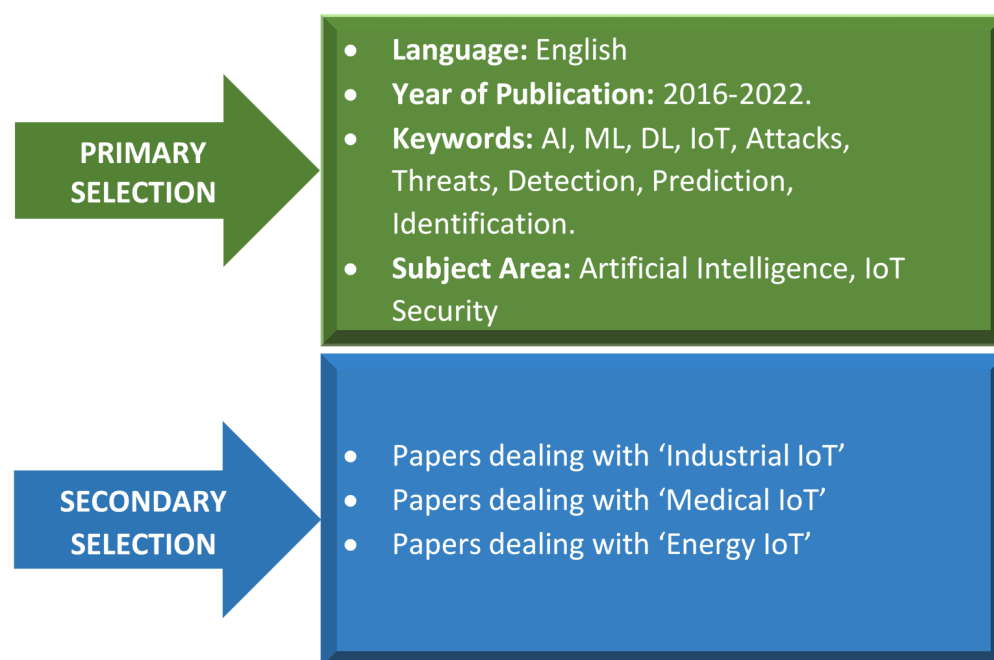


Figure 2. Paper selection procedure.

1.9. Formation of the Remaining Work

The formation of rest of the article is structured as follows: Machine learning methods are described in Section 2. The deep learning methods are comprehensively described in Section 3. Finally, conclusions and future prospects are presented in Section 4.

2. Machine Learning Methods

Different types of machine learning methods have been used for the detection of malicious attacks in the literature. The most used machine learning methods are RF, DT, and KNN. The workings of these machine learning methods are provided as follows.

Figure 3 shows the structure of the DT, which splits the root node into nodes and sub-nodes by using multiple algorithms. Decision nodes are split into further sub-nodes and decide for their sub-nodes. Leaf nodes are the nodes that provide the outcomes and are not split into further sub-nodes. A section of an entire tree is called a sub-tree, which includes a decision node and leaf nodes.

KNN is the simplest and most popular ML algorithm that helps an unknown class to identify its neighboring classes so that it can estimate its own class. Figure 4 shows the KNN process, where we have two classes, A and B, and a class with a question mark that needs estimation of its class regardless of labels. The neighborhood of the query instance is three, because there are three instances within the circle. Within the small circle, we have one instance belonging to class A and two instances belonging to class B. As there are more neighbors of the query instance belonging to class B, it will be assigned the class B label.

Random forest (RF) is an ensemble learning method. It consists of multiple decision trees operating together. A number of decision trees, T_1 – T_n , are trained on different samples (with replacement) of the dataset. Each tree from T_1 to T_n individually provides a

class for a query instance, and the class with more votes becomes the final class prediction, as illustrated in Figure 5.

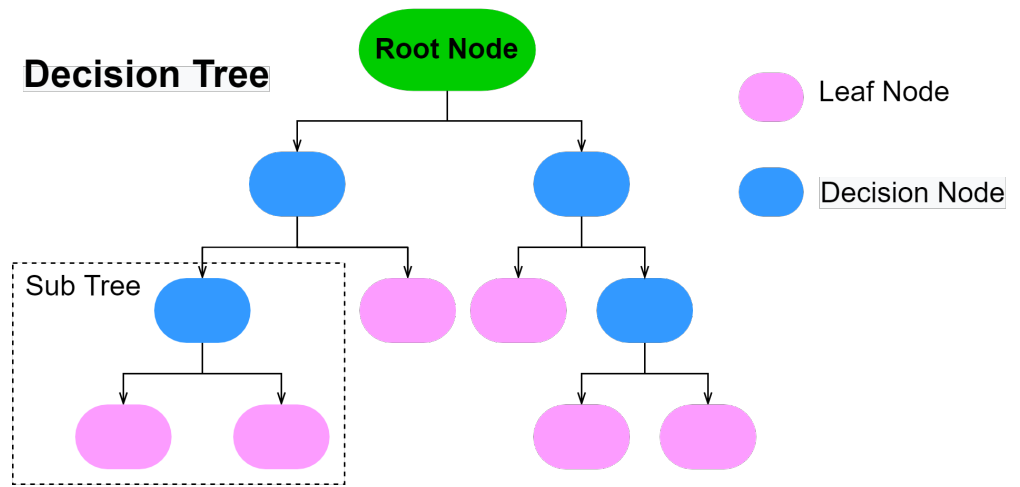


Figure 3. General structure of a decision tree algorithm.

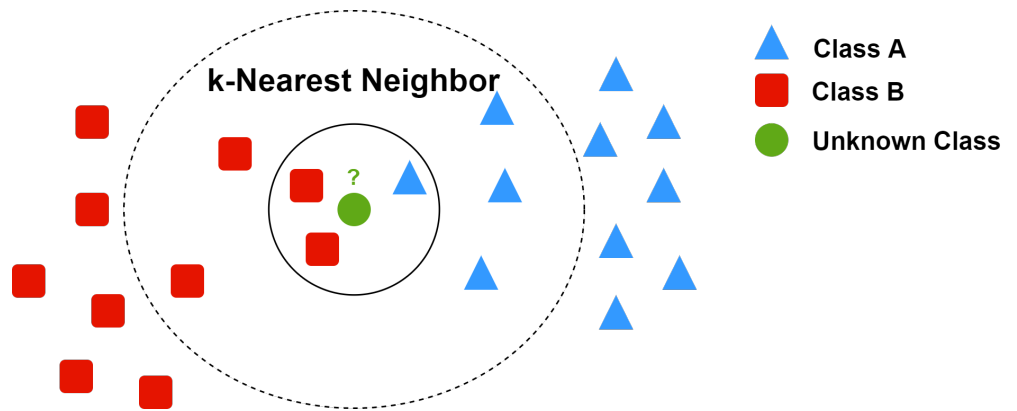


Figure 4. Working structure of a k-nearest neighbors algorithm.

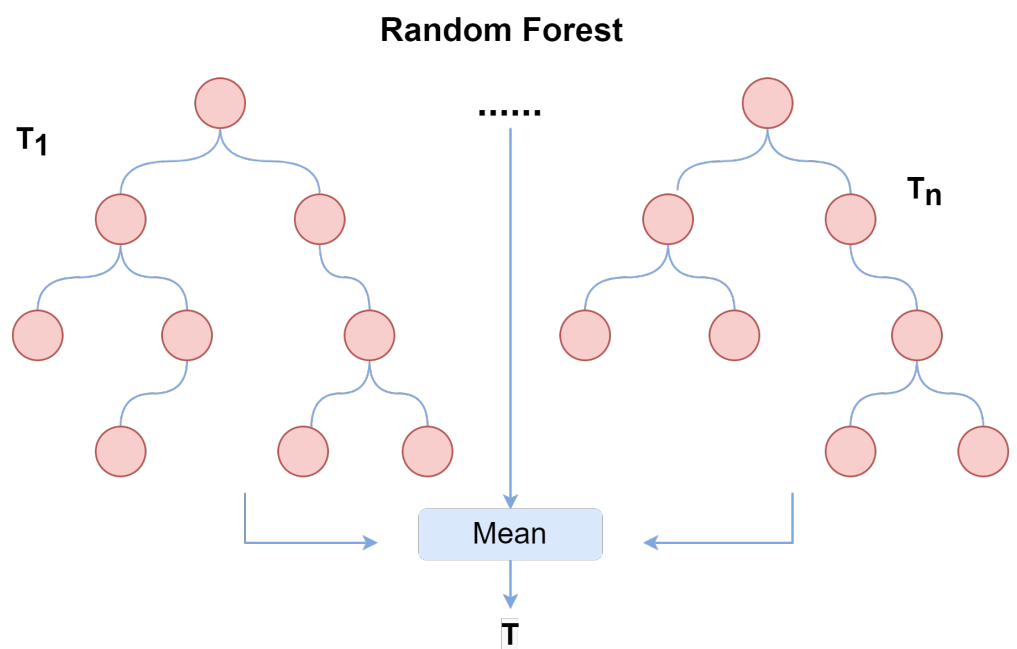


Figure 5. Working structure of a random forest algorithm.

Supervised, semi-supervised, and unsupervised ML methods are presented in the following subsections for detailed discussion on cyber attack detection in IoT systems and devices.

2.1. Supervised Machine Learning Method in IoT Security

An SVM classifier was used in [46] to detect the intrusion of selective forward and blackhole network layer attacks in a network. IoT testbed data were used to test the model against selective forward (SF) and blackhole (BH) attacks. Sink in the middle and at the top network topologies were used to evaluate the detection. The SVM detection model was not able to detect all the malicious nodes for SF attack, and the precision rate was below 50%. The Matthews correlation coefficient equation was used to derive the precision, accuracy, PPV, NPV, and TPR. The results show that 100% TPR and a 99.8% accuracy rate were achieved for SF and BH network routing attacks. In [47], c-support SVM was proposed for detecting abnormalities within IoT networks. Both normal and malicious data were trained and evaluated using the KDD-99 dataset. The detection accuracy was up to 100% when SF and BH attacks were present, whereas 81% detection accuracy was achieved when different network topologies were evaluated for all routing attacks.

A uniform intrusion detection method was used in [48] to detect the intrusions of DoS, probe, U2R, and R2L in an IoT network. To make the IoT network more secure and accurate, NSL-KDD and KDDCUP99 datasets were used, along with random forest as the classifier of supervised machine learning. Other classifiers (KNN, NB, DT, RF, and LR) were used for comparison to test the accuracy of the proposed method. With both the datasets and classifiers, the accuracy of the proposed model was shown to be up to 99.9% with minimum use of time and energy. In [49], researchers proposed the IoTArgos model to detect anomalies and new attacks and to secure the privacy of user data in smart homes. IoTArgos used a two-stage IDS supervised classification algorithm to filter and detect known attacks using a training suite of the classification algorithm. Classifiers used in this article were kNN, LR, RF, NB, and SVM. To identify and evaluate new attacks, IoTArgos also used anomaly detection algorithms of CBLOF, FastABOD, FB, IForest, LOF, and PCA. Experimental result showed that precision rate of proposed IoTArgos model was 0.9876, and its recall rate was 0.9763.

In [50], attacks such as DoS and spoofing were detected using the IoTID20 dataset. RF, SVC, XGBoost, and LR techniques were used to detect intrusion and improve the performance and accuracy of the proposed model. Simulation results showed that these techniques provide high accuracy and can be used to detect IoT attacks. In [51], various supervised ML methods are integrated into the MLLib library of Apache Spark for fast data processing and identification of the SYN-DoS cyber attack. Both performance and application/training time for SYN-DoS cyber attacks were analyzed. Performance and implementation of ML algorithms such as RF, DT, LR, SVM, and GBT were tested on the SYN-DoS public dataset. Experimental results showed that the RF accuracy rate was 100%, and the shortest training time (up to 23.22 s) was achieved for DT, with 2 million rows. The minimum application time was 0.13 s for about 600,000 instances in the case of the RF algorithm with Apache Spark. Note that this algorithm is required to be used in a cloud environment for better scalability and ease of use. Moreover, the model generated by RF is easy-to-use and easy-to-implement in both low and high-level languages. Table 3 presents a summary of different supervised ML methods in terms of: (1) types of malicious attacks, (2) feature selection methods, (3) detection methods, and (4) datasets considered for study.

Table 3. Summary of supervised machine learning methods for cyber attack detection in IoT.

Refs.	Detection Method	Type of Attacks	Feature Selection/Classification Methods	Datasets
[46]	Intrusion Detection	Selective forward and Blackhole network layer attack	SVM	IoTtest bed data
[47]	Anomaly detection	Blackhole, Selective forward, and Sinkhole	c-SVM	KDD-99
[48]	Uniform detection	DoS, U2R, Probe, and R2L	Random Forest	NSL-KDD and KDDCUP99
[49]	IoTArgos	Zero-day or unknown attack	NN, LR, RF, NB, and KNN	
[50]	Intrusion detection	DoS and Spoofing	RF, SVC, and XGBoost	IoTID20
[51]	Mllib of Apache Spark	SYN-DoS attack	RF, DT, LR, SVM, and GBT	SYNDOS2M

2.2. Semi-Supervised Machine Learning Methods in IoT Security

In [52], classifiers such as SVM and KNN were used to classify the feature sets, and ensemble method was used to detect normal or malicious packets. The dataset used in this paper was the NSL-KDD dataset. Note that all classifiers worked in a distributed environment to reduce future attacks. With hybrid methods and fewer features, the accuracy increase was 10%, and the false positive rate was shown to be reduced by 0.05. Hence, it is concluded that detection performance was improved with a higher true positive rate and fewer features. A flow-based NIDS (SSLEEK) approach was developed in [53] to produce alerts on anomaly and malicious attacks. NetFlow files are used to detect botnet traffic in a network session. This method shows improvements in accuracy and efficiency compared to traditional NIDS. The classifiers selected were K-means, K-NN, and GMM. The K-NN classifier is the most popular in machine learning. The workings of the K-NN classifier is shown in Figure 4.

In [54], the hierarchical stacking-temporal convolutional network (HS-TCN) was developed to detect anomalies in the communication of smart homes. Using this semi-supervised technique, a 30% improvement in results was shown as compared to the supervised model. Using hierarchical and stacking methods improves security and performance. A multi-layer clustering model has been proposed in [55] to detect and prevent intrusion. A semi-supervised multi-layered clustering (SMC) model was compared with tri-training and classifiers such as RF, Bagging, and AdaboostM1 with two datasets, NSL and Kyoto 2006+. The results showed that multi-layer clustering performed better than the tri-training model while using 20% less unlabeled data and had comparable performance to the ensemble method, but SMC has a higher testing time than the latter. In [56], fuzziness-based learning approach was used by developing unlabeled samples supported with a supervised approach to improve the performances of classifiers. For a base classifier, NNrw (neural network with random weights) was used because it is computationally efficient and has an excellent learning performance. The proposed method showed that unlabeled samples belong to high and low fuzziness categories, which played an important role in improving the classifiers' performances as compared to other existing classifiers.

In [57], authors proposed a two-model Gaussian fields approach and a spectral graph transducer to detect the unknown malicious attacks. They also used MPCK-means to improve the performances of clustering methods. KDD Cup 1999 dataset was used to test the models. In [58], the DAS-CIDS system was designed to enhance the performance of IDS and to reduce the false alarm rate. The DARPA (KDD99) dataset was used to analyze the performance of the detection, and Snort alarm was used to reduce the false alarm rate. Results showed that the proposed method is more efficient than traditional supervised classifiers due to the automatic support for unlabeled data. A dynamic ensemble algorithm was used in [59] in combination with a semi-supervised extreme learning machine (SSELM). Moreover, the mutual information criterion was proposed for detecting anomalies of large-scale data. SSELM works as a base classifier that provides high relevance and low redundancy. Real-life datasets from UCI (BC, COIL20, ILPD, and HARS) were used for the

experiment, and results showed that the proposed algorithm outperformed the state-of-the-art methods in the case of average classification. In [60], authors proposed the SDRK machine learning model to detect and mitigate intrusion on fog nodes. NSL-KDD was used as a dataset. Testing of SDRK model was performed on fog nodes that lay between cloud layers and IoT. The proposed model showed more accuracy and a shorter testing time. SDRK detection accuracy improves up to 99.78%. Table 4 presents a summary of semi-supervised ML methods in terms of types of malicious attacks, feature selection methods, detection methods, and datasets considered.

Table 4. Summary of semi-supervised machine learning methods for cyber attack detection in IoT.

Refs.	Detection Method	Type of Attacks	Feature Selection/Classification Method	Datasets
[52]	Ensemble-based Learning	Ransomware, DDoS, U2R, and Remote login	RF, SVM, AAN, DT, and KNN	NSL-KDD
[53]	Flow-based, and anomaly-based (SSLEEK)	Botnet traffic, DDoS, and port scanning	K-means, GMM, and KNN	NetFlow files
[54]	HS-TCN	Anomaly detection	KNN, SVM, DT, and Naïve-Bayes	DS2OS
[55]	Multi-Layer Clustering Model	Intrusion Detection and Prevention	RF, Bagging, and AdaboostM1	NSL and Kyoto 2006+
[56]	Fuzziness-based Learning	Intrusion Detection	SVM, RF, and Naïve Bayes	NSL-KDD
[57]	SGT, GFA, and MPCK-means	Signature-based misuse and anomaly detection	Naïve Bayes, Bayes Network, SVM, RF, KNN, C4.5, and RBF Network	KDD Cup 1999
[58]	DAS-CIDS	Enhance intrusion detection and false alarm reduction	KNN, RF, Snort alarm, and J48	KDD99
[59]	Dynamic Ensemble algorithm	Anomaly detection	BC, COIL20, ILPD, and HARS	LapRLS, LapSVM, and SSELN
[60]	SDRK	Detect and Mitigate intrusion, data deluge attack	KNN, DFNN, and RRS- K-means	NSL-KDD

2.3. Unsupervised Learning in IoT Security

The grey wolf optimization one class support vector machine (GWO-OCSVM) was proposed in [61] to detect the botnet attacks that are launched from IoT devices. OCSVM, IF, and LOF algorithms were used to test the proposed model, and results showed that GWO-OCSVM can detect botnet and perform classification better than the other algorithms. With the use of the NN-BaIoT dataset, experiments showed that GWO-OCSVM achieved better results as compared to the other three algorithms in terms of FPR, TPR, and G-means. The performance was enhanced up to 92%. In [62], MCS applications have been used to protect the reliability and correctness of user data. The cyber trustworthiness of the MCS report was ensured in the presence of smart and scheming adversaries. Real IoT datasets are used to prove the effectiveness and accuracy of this model.

In [63], authors proposed the IRESE model to detect rare-events and anomalies on the incoming data stream over the edge devices of IoT. For better detection and performance of the IRESE model, various rare-event types (gunshot, glass break, scream, and siren) were used for testing. The whole system was tested using an agile-based IoT gateway. Testing results proved that IRESE is a portable and lightweight system, which can be deployed anywhere and start detecting rare events from the start. Anomaly-based detection was used in [64] to detect the botnet in IoT devices. Multiple features were used from both datasets (unbalanced and balanced), but only three features were able to differentiate between normal and malicious traffic. Experiments showed the best precision and accuracy of up to 90% were achieved through RF and entropy with five features in both balanced and unbalanced datasets. Note that the result was the same when 10 features were used. Results showed that single model for IoT devices provides better detection. However, a separate model for each IoT device provided a more accurate detection rate.

In [65], authors considered hybrid-based intrusion detection (misuse-based and anomaly-based detection) that uses map reduce for distributed detection. Both misuse and anomaly-based methods used supervised and unsupervised optimum-path forest models to detect the intrusion from wireless sensor network and IoT devices. Anomaly detection based on unsupervised OPF was used for detecting internal attacks that happened in 6LoWAPN, and misuse detection was based on external cyber attacks that happened from the Internet. Both internal and external attack detection showed superior results compared to other existing classifiers.

In [66], authors proposed a network threat situation assessment model using concepts of unsupervised models: it used unlabeled data to detect network threats in an IoT system. CSIC 2010 HTTP, ADFA-LD, UNSW-NB15, and ISOT datasets were used to test the proposed model. Experimental results showed that the developed model performed better than the traditional model based on the supervised method which used labeled data to detect network threats. Table 5 presents a summary of unsupervised ML methods in terms of types of malicious attacks, feature selection methods, detection methods, and datasets considered.

Table 5. Unsupervised machine learning methods for cyber attack detection in IoT.

Refs.	Detection Method	Type of Attacks	Feature Selection/Classification Method	Datasets
[62]	MCS application	Preservation of data trustworthiness	SVM, NN, NB, and RF	Real IoT datasets
[61]	GWO-OCSVM	Botnet detection	LOF, OCSVM, and IF	NN-BaIoT
[63]	IRESE	Anomaly and rare-event detection	Gunshot, glass break, scream, and siren	DCASE 2017 and UrbanSound8k
[64]	Anomaly-based	Botnet attack	LOF, OCSVM, and IF	Unbalanced and balanced
[65]	Hybrid-based detection	Intrusion detection	SVM, NB, and CART	NSL-KDD
[66]	Network Threat Situation Assessment Model (NTSA)	Network Threat	–	CSIC 2010 HTTP, ADFA-LD, UNSW-NB15, and ISOT

3. Deep Learning Methods

Deep learning methods have also been used for detection of malicious attacks in the literature. Popular deep learning methods in the IoT are deep belief networks and adaptive boost algorithms. The deep belief network (DBN) is a popular deep learning algorithm that consists of a visible layer (input Layer) and multiple hidden layers (latent variables). This algorithm works in layers. First, the input layer sends data to the first hidden layer and processes it. Secondly, the next hidden layer takes the first hidden layer as an input layer and processes the data. This process is repeated until the last layer shows the output of the algorithm, which is shown in Figure 6.

Figure 7 presents the working of popular adaptive boost (AdaBoost) algorithm. This algorithm shows that weights are reassigned at each iteration. Higher weights are assigned to an imperfectly classified instance. At the start, all the instances have equal weights. In the first classifier, incorrect classifier instances are given higher weights than corrected classifiers, and these instances are used as an input in the second classifier. This process is repeated until specified conditions are met. In this algorithm, all the classifiers (models) are created by using errors of previous classifiers, and this process repeats until a strong or correct classifier is obtained. The detailed discussions on the use of deep learning for detection of cyber attacks in IoT system are provided in the following.

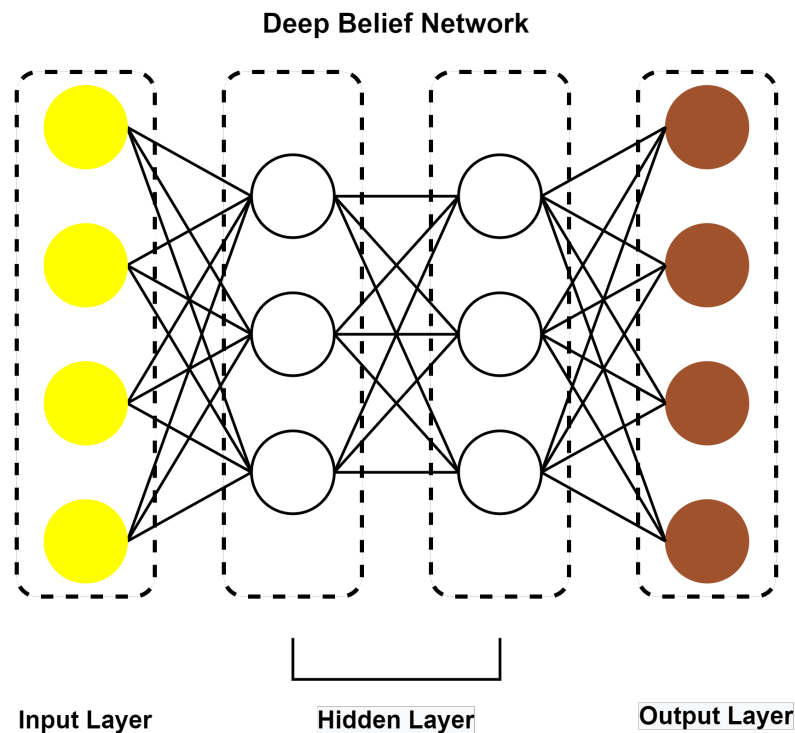


Figure 6. The general structure of a deep belief network.

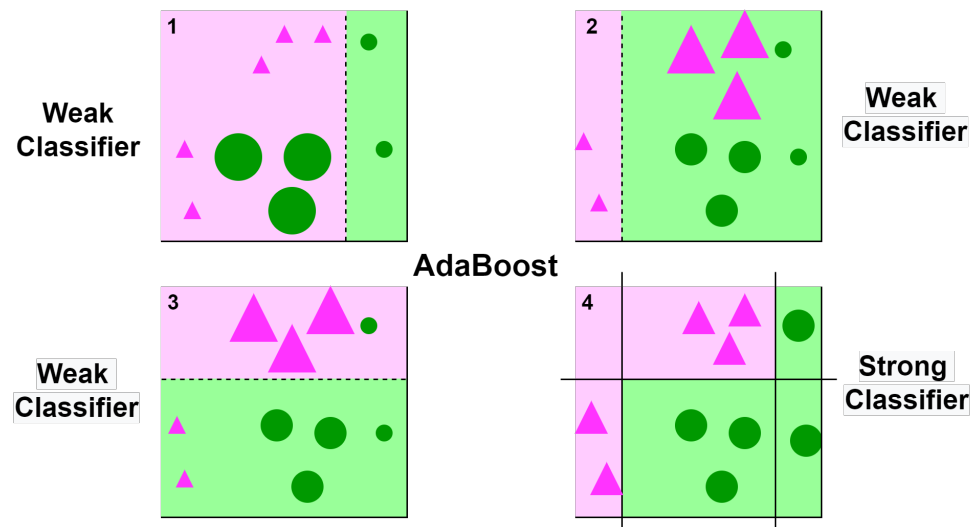


Figure 7. Working of adaptive boost algorithm.

An intrusion detection model based on the hybrid genetic algorithm and deep belief network (DBN) algorithm was presented in [67]. It was achieved higher accuracy and a higher detection rate. For simulation and evaluation of the model, the KDDCUP dataset was utilized. Different existing DL models were used for a performance comparison to detect the intrusion of DoS, R2L, Probe, and U2R attacks. These DL algorithms used for comparison were the thermodynamics-based artificial neural network (TANN), the fuzzy clusters-artificial neural network (FC-ANN), and the back propagation neural network (BPNN). Results showed that the intrusion detection of the hybrid genetic algorithm and DBN model were considerably improved compared to the considered existing DL algorithms. In [68], authors proposed an LM-BP neural-network-based model to detect DoS, R2L, Probe, and U2R attacks. This approach was addressed to prove that it is better than the traditional BP and PSO-BP models. For evaluation, simulation, and performance of this approach, the KDDCUP-99 dataset was utilized. Results showed that LM-BP overpowers

the other models in terms of intrusion detection. Experimental results showed that the false alarm rate is 1.34% and the accuracy rate up to 93.31% better than those of other models.

An IDS model case-sensitive stacked auto-encoder (CSSAE) was developed in [69] to deal with imbalanced data in IDS. Two datasets, KDDCUP-99 and NSL-KDD, were used to evaluate the performance of CSSAE. It was compared with SAE and NDAE models. Experimental results showed that the accuracy of CSSAE is up to 99.35% better and it is 1.15 times faster than SAE and NDAE models. A cyber attack detection method based on the recurrent neural network (RNN) was developed in [70]. LSTM acts as a module in an ensemble of detectors, and LSTM modules merge with DT method to produce the final output. RF, KNN, MLP, and SVM classifiers were applied to the datasets. The effectiveness and performance of the proposed method were evaluated by a real-world dataset (Modbus Network Traffic) and the method obtained a 99% accuracy rate to detect cyber attack in IoT devices.

In [71], a CNN-based dual deep learning model was proposed for disaggregation and aggregation architecture using an energy audit to detect the cyber-physical attack. By using an energy meter, the proposed model checks the system behavior to detect the attacks. The disaggregation model detects a cyber attack, and the aggregation model detects a physical attack. By using energy consumption, the proposed model can detect attacks much better than a single deep learning method. The simulation results showed that a cyber attack is detected in between 900 and 1100 s, and physical attacks are detected in the time frame of 150 to 600 s.

The intelligent intrusion detection system (IID) was used with a DBN-based deep learning algorithm in [72] to detect malicious traffic in an IoT environment. The proposed method was evaluated for both real (provide proof of concept) and simulation (provide evidence of scalability) networks to prove its effectiveness. For evaluation, IID was compared with the inverse weight clustering (IWC) model. Results showed that the proposed model can efficiently detect both real and simulation traffic attacks. IoT devices are changing rapidly in shape, size, complexity, and usage nowadays; and it is getting difficult to detect attacks transferred between IoT devices. Hence, a hybrid convolutional neural network model (HCNN) was developed in [73] to detect the DoS, sinkhole, and eavesdropping attacks in IoT devices. The UNSW NB15 dataset was used, and the RNN model was compared with HCNN for performance comparison. Experimental results showed that the hybrid approach can detect a wider range of attacks in IoT systems than RNN. HCNN achieved 98% better efficiency than RNN.

In [24], a distributed deep learning was proposed for an IoT/Fog system to detect DoS, R2L, Probe, and U2R-based cyber attacks. Distributed deep learning was compared with centralized learning for analysis, and results showed that a distributed deep method can detect attacks with up to 99% accuracy. The NSL-KDD dataset was used to detect attacks in this study. In [74], a deep neural network-based learning strategy was proposed for identification and detection of malicious attacks in IoT networks. The malicious attacks considered were DoS, probing, malicious, scan, spying, wrong setup, and normal attacks in IoT network. Different ML classifiers, GaussianNB, SVM, SDG, RF, LDA, LR, and DT, were compared with DNN on the DS2OS dataset. Simulation results showed that the accuracy rate of training was 98.27% and the testing accuracy rate was 98.29%, which resulted in an average accuracy rate of 98.28%.

A DNN-based framework was proposed in [75] for detecting network attacks and reducing the false alarm rate. The self-adaptive identification method was adopted in which the proposed model can send an early warning in a case of attack detection in an IoT network. For evaluation of performance, the NSL-KDD dataset was used. The early warning accuracy of the proposed DNN model was 99.9% compared to PCA, Gain Ratio, and DBN-based frameworks. SVM and SDA methods were used for attack classification. In [76], a vector convolutional deep learning (VCDL) approach under a fog environment was used to detect DDoS, DoS, theft, and reconnaissance-based malicious attacks in IoT traffic. For testing and evaluation of the model, UNSW's Bot-IoT dataset was used. The

proposed model was compared with SVM, RNN, and LSTM models for performance analysis. Results showed that VCDL performed best, with accuracy, precision, and recall of up to 99.974%, 99.99%, and 99.75%, respectively.

In [77], software defined network–IoT was proposed along with a fuzzy neural network (FNN) to detect three attacks, namely, man-in-the-middle (MITM), malicious code (MC), and side-channel (SC) attacks, in addition to DDoS in IoT traffic. The fuzzy-rule based neural network system was used to test and train the model using the NSL-KDD dataset. With the FNN detection model, the detection accuracy for these four malicious attacks was reported to be up to 83%. In [78], a feed-forward neural network (FFNN) model was proposed with new layers for multi-class classification to detect DDoS, DoS, data gathering, and data theft attacks. The efficiency of the model was tested using both binary and multi-class classification on datasets with real IoT traffic. Results showed that binary classifiers detection accuracy was up to 99.99% and multi-class classifier detection accuracy was 99.79% for the proposed model.

With the rapid growth of IoT devices, it has become more difficult to secure them against malware. In this regard, an ARM-processor-based IoT application was considered in [79]. This processor used an LSTM-based RNN structure to detect malware in IoT network. The LSTM structure had three layers, and it showed promising results compared to RF, NB, SVM, MLP, KDD, DT, and AdaBoost classifiers. The detection accuracy rate was up to 98%. In [80], a bi-directional LSTM recurrent neural network (BLSTM-RNN) model was developed to detect backdoor, DoS, worm, analysis, and reconnaissance attacks in an IoT network, and the UNSW-NB15 dataset was used for evaluation. Experimental results showed that the intrusion detection accuracy rate of proposed method was 95.7%. Moreover, its precision rate and minimum wrong detection rate were 100% and 0.04%, respectively. A zero false alarm rate was also achieved with recall. The f1-score rate was up to 98%.

An anomaly detection system (ADS) based on deep learning was presented in [81] to identify malicious activities, such as fuzzers, analysis, backdoor, DoS, generic, exploits, reconnaissance, shellcode, and worms attacks, in an industrial IoT environment. In the proposed ADS, results of deep auto encoder (DAE) were used for initialization of deep feed-forward neural network (DFNN) in the training phase and testing phase. Old NSL-KDD and new UNSW-NB15 datasets were used to detect both outdated and new malicious attacks. Activities were detected by using DAE and DFNN, two models of ADS, for evaluation. Results showed that the proposed model detection rate was up to 99%, and the false positive rate was minimal, at 1.8%.

In [82], an efficient intrusion detection model was proposed based on deep learning to detect DoS, injection, reconnaissance, and zero-attacks in the Brownfield industrial IoT system. A denoising auto-encoder was used for unsupervised learning from data and a deep neural network for supervised learning from data with the dataset MODBUS. The proposed model was compared with SVM, KNN, NB, and RF models for testing and evaluation. The proposed model showed promising results with a detection rate of 91.49%, a precision rate of 96.41%, and a false positive rate of 1.87%. Table 6 presents a summary of DL methods in terms of types of malicious attacks, feature selection methods, detection methods, and datasets considered.

Table 6. Deep learning methods for cyber attack detection in IoT.

Refs.	Detection Method	Type of Attacks	Feature Selection/Classification Methods	Datasets
[67]	Deep belief network (DBN) and genetic algorithm (GA)	DoS, R2L, Probe, and U2R	TANN, FC-ANN, SA-DT-SVMS, and BPNN	KDDCUP
[68]	LM-BP neural network model	DoS, R2L, Probe, and U2R	Traditional BP and PSO-BP	KDDCUP99
[69]	CSSAE	DoS, R2L, Probe, and U2R	SAE and NDAE	KDDCUP99 and NSL-KDD

Table 6. Cont.

Refs.	Detection Method	Type of Attacks	Feature Selection/Classification Methods	Datasets
[70]	Ensemble, LSTM module	cyber attack	RF, KNN, MLP, and SVM	Modbus network traffic
[71]	Dual deep learning model (energy audit & analytics mechanism)	Cyber and physical attacks	-	-
[72]	Intelligent intrusion detection system	DDoS, sinkhole, blackhole, wormhole, and opportunistic attack	IWC	-
[73]	Hybrid convolutional neural network model (HCNN)	DoS, sinkhole, and eavesdropping	RNN	UNSW-NB15
[24]	Distributed attack detection	DoS, R2L, Probe, and U2R	Duration, protocols, source bytes, destination bytes, service, and flags	NSL-KDD
[74]	DNN based anomaly detection framework	DoS, probing, malicious, scan, spying, wrong setup, and normal attacks	GaussianNB, SVM, SDG, RF, LDA, LR, and DT	DS2OS
[75]	DNN	Network attacks	SVM and SDA	NSL-KDD
[76]	VCDL	DDoS, DoS, theft, and reconnaissance	SVM, RNN, and LSTM	UNSW's Bot-IoT
[77]	SDN-IoT and FNN	MITM, DDoS, side-channel, and malicious code	-	NSL-KDD
[78]	FNN	DoS, DDoS, data gathering, and data theft	SVM	Cutting-edge IoT
[79]	ARM-based IoT and LSTM	Malware threat	RF, NB, SVM, MLP, KDD, DT, and AdaBoost	-
[80]	BLSTM-RNN	Backdoor, DoS, worm, analysis, and reconnaissance	LSTM	UNSW-NB15
[81]	ADS-based deep learning	Fuzzers, analysis, backdoor, DoS, generic, exploits, reconnaissance, shellcode, and worms	F-SVM, DMM, CVT, DBN, RNN, TANN, DNN, and ensemble-DNN	NSL-KDD and UNSW-NB15
[82]	DAE and DNN	DoS, injection, reconnaissance, and zero-attacks	SVM, KNN, NB, and RF	MODBUS

4. Conclusions and Future Prospects

IoT is an emerging technology, but the security of its devices and systems is a major concern. Therefore, this paper presented security concerns on IoT networks. Moreover, supervised, semi-supervised, and unsupervised machine learning methods were discussed for the detection of different malicious attacks in IoT networks. Deep-learning-based methods were also explained for the detection of cyber attacks in IoT systems. In machine and deep learning detection methods, various malicious attacks, such as DoS, DDoS, probing, U2R, R2L, botnet, spoofing, and MITM attacks, were discussed. Moreover, datasets used in machine and deep learning detection methods were also included. All learning methods were compared in terms of the types of attack, feature selection methods, method(s) used to detect attacks, and datasets to pick the best techniques or methods to detect these attacks.

In the future, research should be focused on system throughput, as more IoT devices will be connected to IoT systems. Therefore, scalability issues of detection methods should also be considered when addressing security protocols. Security protocols should be designed to be cost-efficient and computationally efficient to meet the devices' resource constraints. Future studies should also be focused on data security, infrastructure problems, and privacy leakage. Novel machine and deep learning methods can also be explored to overcome cyber attacks. Semi-supervised machine learning and reinforcement learning methods have not been well explored for malicious attack detection in IoT systems. There

is also a need for a comprehensive cyber-detection system which can offer robustness, scalability, accuracy, and protection against all types of malicious threats.

Author Contributions: Conceptualization, U.I., M.F.Z. and M.B.; methodology, U.I. and M.F.Z.; formal analysis, U.I., M.F.Z. and S.M.; investigation, U.I., M.F.Z. and H.M.K.; resources, U.I. and M.F.Z.; data curation, U.I. and M.F.Z.; writing—original draft preparation, U.I., M.F.Z. and S.M.; writing—review and editing, U.I., S.M., H.M.K. and M.B.; supervision, M.F.Z., S.M., H.M.K. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADS	Anomaly detection system
ANN	Artificial neural network
BH	Blackhole
BPNN	Back propagation neural network
CBLOF	Clustering-based local outlier factor
CNN	Convolutional neural network
DT	Decision tree
DBN	Deep belief network
DL	Deep learning
DoS	Denial of service
DDoS	Distributed denial of service
Fast-ABOD	Fast-angle based outlier detection
FC-ANN	Fuzzy clusters artificial neural network
FNN	Fuzzy neural network
Gaussian NB	Gaussian naive bayes
GBT	Gradient boosted tree
IDS	Intrusion detection system
IDT	Intrusion detection threat
IForest	Isolation forest
KNN	K-nearest neighbour
LDA	Linear discriminant analysis
LOF	Local outlier factor
LR	Logistic regression
ML	Machine learning
MC	Malicious code
MITM	Man-in-the-middle
NB	Naive bayes
NPV	Negative predictive value
PPV	Positive predictive value
PCA	Principal component analysis
RF	Random forest
RNN	Recurrent neural network
SC	Side-channel
SF	Selective forward
SH	Sinkhole
SGD	Stochastic gradient descent
SMLC	Semi-supervised multi-layered clustering
SSELM	Semi-supervised extreme learning machine

SVM	Support vector machine
TANN	Thermodynamics-based artificial neural network
TPR	True positive rate
XGBoost	Extreme gradient boosting

References

- Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. *Wirel. Pers. Commun.* **2011**, *58*, 49–69. [\[CrossRef\]](#)
- Elbouchikhi, E.; Zia, M.F.; Benbouzid, M.; El Hani, S. Overview of signal processing and machine learning for smart grid condition monitoring. *Electronics* **2021**, *10*, 2725. [\[CrossRef\]](#)
- Khalid, H.M.; Peng, J.C.H. A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. *IEEE Trans. Smart Grid* **2016**, *7*, 2026–2037. [\[CrossRef\]](#)
- Khalid, H.M.; Muyeen, S.; Peng, J.C.H. Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach. *IEEE Syst. J.* **2019**, *14*, 2054–2065. [\[CrossRef\]](#)
- Souza, L.F.D.F.; Silva, I.C.L.; Marques, A.G.; Silva, F.H.D.S.; Nunes, V.X.; Hassan, M.M.; Albuquerque, V.H.C.D.; Filho, P.P.R. Internet of medical things: An effective and fully automatic IoT approach using deep learning and fine-tuning to lung CT segmentation. *Sensors* **2020**, *20*, 6711. [\[CrossRef\]](#) [\[PubMed\]](#)
- Zia, M.F.; Elbouchikhi, E.; Benbouzid, M.E.H. An Energy Management System for Hybrid Energy Sources-based Stand-alone Marine Microgrid. *IOP Conf. Ser. Earth Environ. Sci.* **2019**, *322*, 012001. [\[CrossRef\]](#)
- Mahmoud, M.S.; Khalid, H.M.; Hamdan, M.M. *Cyberphysical Infrastructures in Power Systems: Architectures and Vulnerabilities*; Elsevier: Amsterdam, The Netherlands, 2021.
- Kiran, D. Chapter 35—internet of things. In *Production Planning and Control*; Kiran, D., Ed.; Butterworth-Heinemann: Oxford, UK, 2019; pp. 495–513.
- Sharma, N.; Shamkuwar, M.; Singh, I. The history, present and future with IoT. In *Internet of Things and Big Data Analytics for Smart Generation*; Springer International Publishing: Cham, Switzerland, 2019; pp. 27–51.
- Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [\[CrossRef\]](#)
- Abbasi, M.A.; Zia, M.F. Novel TPPO based maximum power point method for photovoltaic system. *Adv. Electr. Comput. Eng.* **2017**, *17*, 95–100. [\[CrossRef\]](#)
- Ashraf, S.; Shawon, M.H.; Khalid, H.M.; Muyeen, S. Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. *Sensors* **2021**, *21*, 6415. [\[CrossRef\]](#)
- Khalid, H.M.; Peng, J.C.H. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. *IEEE Trans. Smart Grid* **2017**, *8*, 697–707. [\[CrossRef\]](#)
- Khan, H.M.A.; Inayat, U.; Zia, M.F.; Ali, F.; Jabeen, T.; Ali, S.M. Voice over internet protocol: Vulnerabilities and assessments. In Proceedings of the International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 9–10 November 2021; pp. 1–6.
- Alsharif, M.; Rawat, D.B. Study of Machine Learning for Cloud Assisted IoT Security as a Service. *Sensors* **2021**, *21*, 1034. [\[CrossRef\]](#) [\[PubMed\]](#)
- Choi, C.; Choi, J. Ontology-based security context reasoning for power IoT-cloud security service. *IEEE Access* **2019**, *7*, 110510–110517. [\[CrossRef\]](#)
- Ge, C.; Susilo, W.; Liu, Z.; Xia, J.; Szalachowski, P.; Fang, L. Secure keyword search and data sharing mechanism for cloud computing. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2787–2800. [\[CrossRef\]](#)
- Ge, C.; Susilo, W.; Baek, J.; Liu, Z.; Xia, J.; Fang, L. A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds. *IEEE Trans. Dependable Secur. Comput.* **2021**, *1*. [\[CrossRef\]](#)
- Ge, C.; Susilo, W.; Baek, J.; Liu, Z.; Xia, J.; Fang, L. Revocable attribute-based encryption with data integrity in clouds. *IEEE Trans. Dependable Secur. Comput.* **2021**, *1*. [\[CrossRef\]](#)
- Ge, C.; Liu, Z.; Xia, J.; Fang, L. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1214–1226. [\[CrossRef\]](#)
- La, Q.D.; Quek, T.Q.S.; Lee, J.; Jin, S.; Zhu, H. Deceptive attack and defense game in honeypot-enabled networks for the internet of things. *IEEE Internet Things J.* **2016**, *3*, 1025–1035. [\[CrossRef\]](#)
- Han, X.; Kheir, N.; Balzarotti, D. Deception techniques in computer security: A research perspective. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–36. [\[CrossRef\]](#)
- Inayat, U.; Zia, M.F.; Ali, F.; Ali, S.M.; Khan, H.M.A.; Noor, W. Comprehensive review of malware detection techniques. In Proceedings of the International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 9–10 November 2021; pp. 1–6.
- Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for internet of things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [\[CrossRef\]](#)
- Lin, T. Deep learning for IoT. In Proceedings of the IEEE 39th International Performance Computing and Communications Conference (IPCCC), Austin, TX, USA, 6–8 November 2020; pp. 1–4.
- McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.

27. 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.
28. Tama, B.A.; Rhee, K.H. Attack classification analysis of IoT network via deep learning approach. *Res. Briefs Inf. Commun. Technol. Evol. (ReBICTE)* **2017**, *3*, 1–9.
29. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [[CrossRef](#)]
30. 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](#)]
31. Parra, G.D.L.T.; Rad, P.; Choo, K.K.R.; Beebe, N. Detecting internet of things attacks using distributed deep learning. *J. Netw. Comput. Appl.* **2020**, *163*, 102662. [[CrossRef](#)]
32. Fu, Y.; Yan, Z.; Cao, J.; Koné, O.; Cao, X. An automata based intrusion detection method for internet of things. *Mob. Inf. Syst.* **2017**, *2017*, 1750637. [[CrossRef](#)]
33. Otoum, Y.; Liu, D.; Nayak, A. DL-IDS: A deep learning-based intrusion detection framework for securing IoT. *Trans. Emerg. Telecommun. Technol.* **2019**, *33*, e3803. [[CrossRef](#)]
34. Idrissi, I.; Boukabous, M.; Azizi, M.; Moussaoui, O.; El Fadili, H. Toward a deep learning-based intrusion detection system for IoT against botnet attacks. *IAES Int. J. Artif. Intell.* **2021**, *10*, 110. [[CrossRef](#)]
35. Shafiq, M.; Tian, Z.; Bashir, A.K.; Du, X.; Guizani, M. CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet Things J.* **2020**, *8*, 3242–3254. [[CrossRef](#)]
36. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for consumer internet of things devices. In Proceedings of the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35.
37. Stiawan, D.; Arifin, M.A.S.; Idris, M.Y.; Budiarto, R. IoT botnet malware classification Using Weka Tool and scikit-learn machine learning. In Proceedings of the 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia, 1–2 October 2020; pp. 15–20.
38. Mohamed, T.; Otsuka, T.; Ito, T. Towards machine learning based IoT intrusion detection service. In Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Montreal, QC, Canada, 25–28 June 2018; pp. 580–585.
39. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [[CrossRef](#)]
40. Rezaei, A. Detecting botnet on IoT by using unsupervised learning techniques. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)* **2020**, *18*, 89–100.
41. Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A survey of deep learning methods for cyber security. *Information* **2019**, *10*, 122. [[CrossRef](#)]
42. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [[CrossRef](#)]
43. 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](#)]
44. 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](#)]
45. Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep learning and big data technologies for IoT security. *Comput. Commun.* **2020**, *151*, 495–517. [[CrossRef](#)]
46. Ioannou, C.; Vassiliou, V. Experimentation with local intrusion detection in IoT networks using supervised learning. In Proceedings of the 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, 25–27 May 2020; pp. 423–428.
47. Ioannou, C.; Vassiliou, V. Classifying security attacks in IoT networks using supervised learning. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 652–658.
48. Rani, D.; Kaushal, N.C. Supervised machine learning based network intrusion detection system for internet of things. In Proceedings of the 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–7.
49. Wan, Y.; Xu, K.; Xue, G.; Wang, F. Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 874–883.
50. Krishnan, S.; Neyaz, A.; Liu, Q. IoT network attack detection using supervised machine learning. *Int. J. Artif. Intell. Expert Syst.* **2021**, *10*, 18–32.
51. Morfino, V.; Rampone, S. Towards near-real-time intrusion detection for IoT devices using supervised learning and APACHE Spark. *Electronics* **2020**, *9*, 444. [[CrossRef](#)]
52. Khonde, S.; Ulagamuthalvi, V. Ensemble-based semi-supervised learning approach for a distributed intrusion detection system. *J. Cyber Secur. Technol.* **2019**, *3*, 163–188. [[CrossRef](#)]
53. Leslie, N.O. Using semi-supervised learning for flow-based network intrusion detection. *Cell* **2018**, *202*, 528-0770.

54. Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. HS-TCN: A semi-supervised hierarchical stacking temporal convolutional network for anomaly detection in IoT. In Proceedings of the IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, UK, 29–31 October 2019; pp. 1–7.
55. Al-Jarrah, O.Y.; Al-Hammdi, Y.; Yoo, P.D.; Muhaidat, S.; Al-Qutayri, M. Semi-supervised multi-layered clustering model for intrusion detection. *Digit. Commun. Netw.* **2018**, *4*, 277–286. [[CrossRef](#)]
56. Ashfaq, R.A.R.; Wang, X.Z.; Huang, J.Z.; Abbas, H.; He, Y.L. Fuzziness based semi-supervised learning approach for intrusion detection system. *Inf. Sci.* **2017**, *378*, 484–497. [[CrossRef](#)]
57. Chen, C.; Gong, Y.; Tian, Y. Semi-supervised learning methods for network intrusion detection. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Singapore, 12–15 October 2008; pp. 2603–2608.
58. 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](#)]
59. Liu, S.; Hao, X.; Chen, X. A semi-supervised dynamic ensemble algorithm for IoT anomaly detection. In Proceedings of the International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, 2–6 November 2020; pp. 264–269.
60. Ravi, N.; Shalinie, S.M. Semisupervised-learning-based security to detect and mitigate intrusions in IoT network. *IEEE Internet Things J.* **2020**, *7*, 11041–11052. [[CrossRef](#)]
61. Al Shorman, A.; Faris, H.; Aljarah, I. Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 2809–2825. [[CrossRef](#)]
62. Banerjee, N.; Giannetos, T.; Panaousis, E.; Took, C.C. Unsupervised learning for trustworthy IoT. In Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
63. Janjua, Z.H.; Vecchio, M.; Antonini, M.; Antonelli, F. IRESE: An intelligent rare-event detection system using unsupervised learning on the IoT edge. *Eng. Appl. Artif. Intell.* **2019**, *84*, 41–50. [[CrossRef](#)]
64. Nõmm, S.; Bahşı, H. Unsupervised anomaly based botnet detection in IoT networks. In Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 1048–1053.
65. Sheikhan, M.; Bostani, H. A hybrid intrusion detection architecture for internet of things. In Proceedings of the 8th International Symposium on Telecommunications (IST), Tehran, Iran, 27–28 September 2016; pp. 601–606.
66. Yang, H.; Zeng, R.; Wang, F.; Xu, G.; Zhang, J. An unsupervised learning-based network threat situation assessment model for internet of things. *Secur. Commun. Netw.* **2020**, *2020*, 6656066. [[CrossRef](#)]
67. Li, P.; Zhang, Y. A novel intrusion detection method for internet of things. In Proceedings of the Chinese Control Additionally, Decision Conference (CCDC), Nanchang, China, 3–5 June 2019; pp. 4761–4765.
68. Yang, A.; Zhuansun, Y.; Liu, C.; Li, J.; Zhang, C. Design of intrusion detection system for internet of things based on improved BP neural network. *IEEE Access* **2019**, *7*, 106043–106052. [[CrossRef](#)]
69. Telikani, A.; Gandomi, A.H. Cost-sensitive stacked auto-encoders for intrusion detection in the internet of things. *Internet Things* **2019**, *14*, 100122. [[CrossRef](#)]
70. 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](#)]
71. Li, F.; Shi, Y.; Shinde, A.; Ye, J.; Song, W. Enhanced cyber-physical security in internet of things through energy auditing. *IEEE Internet Things J.* **2019**, *6*, 5224–5231. [[CrossRef](#)]
72. Thamilarasu, G.; Chawla, S. Towards deep-learning-driven intrusion detection for the internet of things. *Sensors* **2019**, *19*, 1977. [[CrossRef](#)]
73. Smys, S.; Basar, A.; Wang, H. Hybrid intrusion detection system for internet of things (IoT). *J. ISMAC* **2020**, *2*, 190–199. [[CrossRef](#)]
74. Reddy, D.K.; Behera, H.S.; Nayak, J.; Vijayakumar, P.; Naik, B.; Singh, P.K. Deep neural network based anomaly detection in internet of things network traffic tracking for the applications of future smart cities. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4121. [[CrossRef](#)]
75. Li, J.; Sun, B. A Network attack detection method Using SDA and deep neural network based on internet of things. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 209–214. [[CrossRef](#)]
76. NG, B.A.; Selvakumar, S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. *Future Gener. Comput. Syst.* **2020**, *113*, 255–265.
77. Farhin, F.; Sultana, I.; Islam, N.; Kaiser, M.S.; Rahman, M.S.; Mahmud, M. Attack detection in internet of things using software defined network and fuzzy neural network. In Proceedings of the Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR), Kitakyushu, Japan, 26–29 August 2020; pp. 1–6.
78. Ge, M.; Syed, N.F.; Fu, X.; Baig, Z.; Robles-Kelly, A. Towards a deep learning-driven intrusion detection approach for internet of things. *Comput. Netw.* **2021**, *186*, 107784. [[CrossRef](#)]
79. HaddadPajouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.K.R. A deep recurrent neural network based approach for internet of things malware threat hunting. *Future Gener. Comput. Syst.* **2018**, *85*, 88–96. [[CrossRef](#)]

80. Roy, B.; Cheung, H. A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network. In Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018; pp. 1–6.
81. Muna, A.H.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* **2018**, *41*, 1–11.
82. Al-Hawawreh, M.; Sitnikova, E.; den Hartog, F. An efficient intrusion detection model for edge system in brownfield industrial Internet of Things. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, Melbourne, Australia, 22–24 August 2019; pp. 83–87.