sensors

IMPACT FACTOR 3.847

Indexed in: PubMed

Review

A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms

Abebe Diro, Naveen Chilamkurti, Van-Doan Nguyen and Will Heyne

Special Issue

Wireless Sensing and Networking for the Internet of Things

Edited by

Prof. Dr. Zihuai Lin and Prof. Dr. Wei Xiang

MDPI

https://doi.org/10.3390/s21248320

sensors

MDPI

Review

A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms

Abebe Diro [1], Naveen Chilamkurti [2], Van-Doan Nguyen [2,*] and Will Heyne [3]

[1] College of Business and Law, RMIT University, Melbourne 3001, Australia; abebe.diro3@rmit.edu.au
[2] Department of Computer Science and I.T., La Trobe University, Melbourne 3086, Australia; n.chilamkurti@latrobe.edu.au
[3] BAE Systems Australia, Adelaide 5000, Australia; will.heyne@baesystems.com
* Correspondence: o.nguyen@latrobe.edu.au

Abstract: The Internet of Things (IoT) consists of a massive number of smart devices capable of data collection, storage, processing, and communication. The adoption of the IoT has brought about tremendous innovation opportunities in industries, homes, the environment, and businesses. However, the inherent vulnerabilities of the IoT have sparked concerns for wide adoption and applications. Unlike traditional information technology (I.T.) systems, the IoT environment is challenging to secure due to resource constraints, heterogeneity, and distributed nature of the smart devices. This makes it impossible to apply host-based prevention mechanisms such as anti-malware and anti-virus. These challenges and the nature of IoT applications call for a monitoring system such as anomaly detection both at device and network levels beyond the organisational boundary. This suggests an anomaly detection system is strongly positioned to secure IoT devices better than any other security mechanism. In this paper, we aim to provide an in-depth review of existing works in developing anomaly detection solutions using machine learning for protecting an IoT system. We also indicate that blockchain-based anomaly detection systems can collaboratively learn effective machine learning models to detect anomalies.

Keywords: cybersecurity; anomaly detection; the Internet of Things; machine learning; deep learning; blockchain

check for updates

Citation: Diro, A.; Chilamkurti, N.; Nguyen, V.-D.; Heyne, W. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. *Sensors* **2021**, *21*, 8320. https://doi.org/10.3390/s21248320

Academic Editors: Zihuai Lin and Wei Xiang

Received: 8 November 2021
Accepted: 8 December 2021
Published: 13 December 2021

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

Copyright: © 2021 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

The IoT consists of myriad smart devices capable of data collection, storage, processing, and communication. The adoption of the IoT has brought about tremendous innovation opportunities in industries, homes, the environment, and businesses, and it has enhanced the quality of life, productivity, and profitability. However, infrastructures, applications, and services associated with the IoT introduced several threats and vulnerabilities as emerging protocols and workflows exponentially increased attack surfaces [1]. For instance, the outbreak of the Mirai botnet exploited IoT vulnerabilities and crippled several websites and domain name systems [2].

It is challenging to secure IoT devices as they are heterogeneous, traditional security controls are not practical for these resource-constrained devices, and the distributed IoT networks fall out of the scope of perimeter security, and existing solutions such as the cloud suffer from centralisation and high delay. Another reason for this challenge is that IoT device vendors commonly overlook security requirements due to a rush-to-market mentality. Furthermore, the lack of security standards has added another dimension to the complexity of securing IoT devices. These challenges and the nature of IoT applications call for a monitoring system such as anomaly detection at device and network levels beyond the organisational boundary.

An anomaly is a pattern or sequence of patterns in IoT networks or data that significantly deviate from the normal behaviour. Anomalies can be contextual and collective

points based on the sources of anomalies [3]. Point anomaly represents a specific data point that falls outside the norm, and it indicates random irregularity, extremum, or deviation with no meaning, often known as outliers. The contextual anomaly denotes a data point that deviates from the norm in a specific context such as in a time window. It means that the same normal observation in a given context can be abnormal in a different context. The contextual anomaly is driven by contextual features such as time and space and behavioural features such as the application domain. A collection of related data points, specifically in sequential, spatial, and graph data, that fall outside of normal behaviour forms collective anomalies. It is denoted as a group of interconnected, correlated, or sequential instances, where individuals of the group are not anomalous themselves; the collective sequence is anomalous. Anomalous events rarely occur; however, these events bring about dramatic negative impacts in businesses and governments using IoT applications [4].

As for protecting IoT and I.T. applications, intrusion detection systems (I.D.S.s) that alert abnormal events or suspicious activities that might lead to an attack have been developed. I.D.S.s can be divided into two main categories: anomaly-based and signature-based. With anomaly-based I.D.S.s, unidentified attacks or zero-day attacks can be detected as deviations from normal activities [5]. However, signature-based I.D.S cannot identify unknown attacks until the vendors release updated versions consisting of the new attack signatures [5]. This indicates that anomaly-based I.D.S.s are strongly positioned to secure IoT devices better than signature-based I.D.S.s. Moreover, there is a large amount of raw data generated by IoT devices, which leads to the process of identifying suspicious behaviour from data suffering from high computation cost due to included noise. Hence, lightweight distributed anomaly-based I.D.S.s play a significant role in thwarting cyber-attacks in the IoT network.

In recent years, using machine learning techniques to develop anomaly-based I.D.S.s to protect the IoT system has produced encouraging results as machine learning models are trained on normal and abnormal data and then used to detect anomalies [1,2]. However, building effective and efficient anomaly detection modules is a challenging task as machine learning has the following drawbacks:

- First, machine learning models, specifically with classical algorithms, are shallow to extract features that can truly represent underlying data to discriminate anomaly events from normal ones.
- Second, running machine learning models can consume extensive resources, making it challenging to deploy such models on resource-constrained devices.
- Third, it requires massive data for training machine learning models to archive high accuracy in anomaly detection. Therefore, machine learning models may not capture all of the cyber-attacks or suspicious events due to training data. This means that machine learning suffers from both false positives and false negatives in some circumstances.

However, with the advancement in hardware such as GPU and neural networks such as deep learning, machine learning has constantly improved. This makes it promising for anomaly detection emerging platforms such as blockchain.

This paper aims to provide an in-depth review of current works in developing anomaly detection solutions using machine learning to protect an IoT system, which can help researchers and developers design and implement new anomaly-based I.D.S.s. Our contributions are summarised as follows: first, we present the significance of anomaly detection in the IoT system (Section 2); then, we identify the challenges of applying anomaly detection to an IoT system (Section 3); after that, we describe the state-of-the-art machine learning techniques for detecting anomalies in the system (Section 4); finally, we analyse the use of machine learning techniques for IoT anomaly detection (Section 5). In particular, this paper also covers the federated learning technique that helps to collaboratively train effective machine learning models to detect anomalies (Section 4) and indicates that the use of blockchain for anomaly detection is a novel contribution as the inherent characteristics of a distributed ledger is an ideal solution to defeat adversarial learning systems (Section 5).

2. Significance of Anomaly Detection in the IoT

Over the years, anomaly-based I.D.S.s have been applied in a wide range of IoT applications, as illustrated in Table 1. This section will focus on the important roles of anomaly detection systems in industries, smart grids, and smart cities.

Table 1. Anomaly-Based I.D.S.s according to Anomaly Types and Applications.

		ANOMALY TYPES		
		Points	**Contextual**	**Collective**
APPLICATIONS	**Generic**	[6] [9]	[7]	[8] [10] [11] [12] [13] [14] [15]
	Flights		[16]	
	Industries	[17] [18] [19]		
	Health		[20]	
	Smart Cities	[21]		
	Smart Grids		[22]	
	Smart Home	[23]		[24] [25] [26]
	Unmanned Aerial Vehicles		[27]	

Industrial IoT is one of the beneficiaries of anomaly detection tools. Anomaly detection has been leveraged for industrial IoT applications such as power systems, health monitoring [28], heating ventilation and air conditioning system fault detection [29], production plant maintenance scheduling [30], and manufacturing quality control systems [31]. In [32], machine learning approaches such as linear regression have been applied to sensor readings of engine-based machines to learn deviations from normal system behaviours. The study demonstrated that anomaly detection plays a significant role in preventive maintenance by detecting machine failures and inefficiencies. In another study, autoencoder (A.E.)-based outlier detection was investigated in audio data using reconstruction error [33]. The study showed that early detection of anomalies could be used as responsive maintenance for machine failures, thereby reducing downtime. Furthermore, water facilities used IoT anomaly detection [34] to monitor and identify certain chemical concentration levels as a reactive alerting mechanism. These studies show that IoT anomaly detection provides mechanisms of improving efficiency and system up-time for industry machines by monitoring machine health.

The power sector including existing smart grids has also attracted anomaly detection systems to identify power faults and outages. The study in [35] utilised statistical methods to develop an anomaly detection framework using smart meter data. The authors argue that hierarchical network data can be used to model anomaly detection for power systems. The other study [36] employed high-frequency signals to detect anomalies in power network faults. The article concludes that local anomaly detection depends more on network size than topology. In [37], big data analysis schemes were explored to detect and localise failures and faults in power systems. The study showed that the compensation theorem in circuit theory could be applied to event detection in power networks. Physical attacks on smart grids such as energy theft can also be detected by using anomaly detection systems,

as shown in [38]. It is compelling that anomaly detection plays a paramount role in detecting failures and faults in power systems, enhancing system reliability and efficiency.

Abnormality detection can be used for smart city facilities such as roads and buildings. Road surface anomalies were studied in [39]. It has been indicated that damage to private vehicles can be reduced if the road surface is monitored for anomalies so that timely measures such as maintenance are taken before road incidents. In the study undertaken in [40], pollution monitoring and controlling were modelled as an anomaly to enable policymaker decisions in health, traffic, and environment. Similarly, assisted living can also benefit from IoT-based anomaly detection as deviations from normal alert caregivers as studied in [41]. Thus, it can be summed up that abnormal situations in smart cities and buildings can be detected using anomaly detection systems, and these can be provided to policymakers for decision-making purposes.

3. Challenges in IoT Anomaly Detection Using Machine Learning

The development of anomaly detection schemes in the IoT environment is challenging due to several factors such as (1) scarcity of IoT resources; (2) profiling normal behaviours; (3) the dimensionality of data; (4) context information; and (5) the lack of resilient machine learning models [15]. These factors will be explained in this section.

3.1. Scarcity of IoT Resources

The leverage of device-level IoT anomaly detection can be hindered by the constraints in storage, processing, communication, and power resources. To compensate for this, the cloud can be adopted as a data collection, storage, and processing platform. However, the remoteness of the cloud can introduce high latency due to resource scheduling and round trip time. This delay may not be acceptable for real-time requirements of IoT suspicious events [15]. It is also evident that the scale of traffic in the IoT may degrade the detection performance of the anomaly detection system if it exceeds the capacity of the devices. A better solution is to offload certain storage and computations from devices to edge nodes or to send aggregated data to the cloud. Sliding window techniques can also offer reduced storage benefits by withholding only certain data points, though the anomaly detection system may require patterns/trends [26].

3.2. Profiling Normal Behaviours

The success of an anomaly detection system depends on gathering sufficient data about normal behaviours; however, defining normal activities is challenging. Due to their rare occurrence, anomalous behaviours might be collected within normal behaviours. There is a lack of datasets representing both IoT normal and abnormal data, making supervised learning impractical, specifically for massively deployed IoT devices. This drives the need to model IoT anomaly detection systems in unsupervised or semi-supervised schemes, where data deviating from those collected in normal operations are taken as anomalous [3].

3.3. Dimensionality of Data

IoT data can be univariate as key-value x_t or multivariate as temporally correlated univariate $x_t = \left[{x_t}^1, \ldots, {x_t}^n\right]$. The IoT anomaly detection using univariate series compares current data against historical time series. In contrast, multivariate-based detection provides historical stream relationships and relationships among attributes at a given time. Thus, choosing a specific anomaly detection mechanism in IoT applications depends on data dimensionality due to associated overheads in processing [3,29]. Furthermore, multivariate data introduces the complexity of processing for models, which needs dimension reduction techniques using principal components analysis (P.C.A.) and A.E.s. On the other hand, univariate data may not represent finding patterns and correlations that enhance machine learning performance.

3.4. Context Information

The distributed nature of IoT devices caters to context information for anomaly detection. However, the challenge is to capture the temporal input at a time t_1 is related to input at a time t_n and spatial contexts in large IoT deployments where some IoT devices are mobile in their operations. This means that introducing context enriches anomaly detection systems, but increases complexity if the right context is not captured [3].

3.5. Lack of Machine Learning Models Resiliency against Adversarial Attacks

The lack of a low false-positive rate of existing machine learning models and the vulnerability to adversarial attacks during training and detection call for both accurate algorithms and resilient models. On the other hand, the massive deployment of IoT devices could be leveraged for collective anomaly detection as most of the devices in the network exhibit similar characteristics. This large number of devices helps to utilise the power of cooperation against cyber-attacks such as malware [42]. Model poisoning and evasion can decrease the utility of machine learning models as adversaries can introduce fake data to train or tamper the model.

4. Machine Learning Techniques for Detecting Anomalies in the IoT

Several aspects of IoT anomaly detection using machine learning must be considered. Learning algorithm methods can be categorised into three groups: supervised, unsupervised, and semi-supervised. The technique to train the learning algorithms across many decentralised IoT devices is known as federated learning. In addition, anomaly detection can be seen in terms of extant data dimension, leading to univariate-and multivariate-based approaches. In the rest of this section, we will present the anomaly detection schemes based on (1) machine learning algorithms; (2) federated learning; and (3) data sources and dimensions.

4.1. Detection Schemes Based on Machine Learning Algorithms

Supervised algorithms, known as discriminative algorithms, are classification-based learning through labelled instances. These algorithms consist of classification algorithms such as the K-nearest neighbour (K.N.N.), support vector machine (SVM), Bayesian network, and neural network (N.N.) [43,44]. K.N.N. is one of the distance-based algorithms of anomaly detection where the distances of anomalous points from the majority of the dataset are greater than a specific threshold. Calculating the distances is computationally complex; it seems impossible to provide on-device anomaly detection using this algorithm. On the other hand, SVM provides a hyperplane that divides data points for classification. As in the case of K.N.N., it is so resource-intensive that the applicability to IoT anomaly detection is impractical. As the Bayesian network may not require the prior knowledge of neighbour nodes for anomaly detection, it can be adopted for resource-constrained devices through low accuracy. Finally, N.N. algorithms have been extensively used to train on normal data so that anomalous data can be detected as the deviation from normal. The resource requirements of N.N. algorithms make it challenging to adapt to the IoT environment. Hence, supervised algorithms are the least applicable for IoT anomaly detection systems for their labelled dataset requirements and extensive resource requirements.

Commonly known as generative algorithms, unsupervised algorithms use unlabelled data to learn hierarchical features. Clustering-based algorithms such as K-means and density-based spatial clustering of applications with noise (D.B.S.C.A.N.) are unsupervised techniques that apply similarity and density attributes to classify data points into clusters [43,44]. Abnormal points are small data points significantly far from the dense area, while normal points are either close to or within the clusters. Usually, clustering algorithms are used with classification algorithms to enhance anomaly detection accuracy. Because of resource usage, most of the clustering algorithms cannot be directly applied to IoT devices for anomaly detection. Another unsupervised learning technique involves dimension-reduction approaches such as P.C.A. and A.E. to remove noise and redundancy from data

to reduce the dimension of original data [44,45]. P.C.A. has been extensively applied to anomaly detection, but it fails in the dynamic IoT environment. A.E. has produced promising results in IoT anomaly detection in reducing data sizes and in reconstructing errors to identify anomalous points. However, these techniques have been used extensively as a part of feature extraction for classification algorithms. The dimensionality reduction algorithms in unsupervised learning can be adapted to IoT anomaly detection. Semi-supervised algorithms combine discriminative and generative algorithms by providing normal data instances so that deviation from normal behaviour is seen as abnormal behaviour. Hence, anomaly detection in IoT is geared toward unsupervised or semi-supervised algorithms where normal system profiling is utilised as a baseline environment [46].

Table 2 shows the state-of-the-art machine learning algorithms according to three anomaly types.

Table 2. Learning Algorithms According to Anomaly Types and Machine Learning Schemes.

		ANOMALY TYPES		
		Points	**Contextual**	**Collective**
MACHINE LEARNING SCHEMES	**Supervised**	RF [21] DL [17]	RL [16] LSTM [22]	CNN [24] GNN [8] Multiple [10] AE-ANN [11] LSTM [12] AE-CNN [13] Ensemble [14]
	Unsupervised	AE-CNN [6] AE [18]	Subspace [27]	AE [25] Self-learning [26]
	Semi-Supervised	TCN [23]	AE-LSTM [20] DBN [7]	DNN [15]

4.2. Training Detection Schemes Based on Federated Learning Algorithms

Federated learning, also known as collaborative learning, allows IoT devices to train machine learning models locally and send the trained models, not the local data, to the server for aggregation [47,48]. This training method is different from the standard machine learning training approaches that require centralising the training data in one place such as a server or data centre.

The federating learning method consists of four main steps. First, the server initialises a global machine learning model for anomaly detection and selects a subset of IoT devices to send the initialised model. Second, each selected IoT device will train the model by using its local data, then send the trained model back to the server. Next, the server will aggregate received models to form the global model. Finally, the server will send the final model to all IoT devices to detect anomalies. Note that the server can repeat the tasks of selecting a sub-set of IoT devices, sending the global model, receiving the trained models, and aggregating the received models multiple times, as some devices may not be available at the time of federated computation or some may have dropped out during each round.

By using federated learning, data in the IoT system is decentralised, and data privacy is protected. The other advantages of federated learning include lower latency, less network load, less power consumption, and can be applied across multiple organisations. However, federated learning also suffers from some drawbacks such as inference attacks [49] and model poisoning [50].

4.3. Detection Mechanisms Based on Data Sources and Dimensions

Univariate IoT data consists of data representation from a single IoT device over time. In reality, anomaly detection systems utilise data from multiple IoT devices deployed in complex environments. These multivariate multi-sources feed richer contexts by providing noise-tolerant temporal and spatial information than a single source.

4.3.1. Univariate Using Non-Regressive Scheme

In the non-regressive scheme, threshold-based mechanisms can be leveraged by setting low and high thresholds of observations on univariate stationary data to flag anomalies if a data point falls outside the boundary. More advanced mechanisms such as mean and variance thresholds produced over historical data can replace this min–max approach. Another similar approach is using a box plot to split data distribution into a range of small categories where new data points are compared against the boxes. These non-regressive approaches are ideal in saving resources such as processors and memories for IoT devices. However, being distributed techniques over univariate observations, the range-based schemes fail to detect contextual and collective anomalies due to the lack of the ability to capture temporal relationships [3].

N.N.s such as A.E.s, recurrent neural networks (R.N.N.), and long short-term memory (L.S.T.M.) can be used as non-regressive models to solve the problem of anomaly detection in the IoT ecosystem using univariate time series data. A.E. is used to reconstruct data symmetrically from the input to the output layer, and a high reconstruction error probably indicates abnormality [13]. A.E. can also be applied to resource-constrained IoT devices for conserving resources and battery power. On the other hand, R.N.N. provides memory in the network by affecting neurons from previous outputs through feedback loops. This enables the capture of temporal contexts over time. The vanishing gradient problem in R.N.N. makes it unsuitable for large IoT networks. L.S.T.M. can provide semi-supervised learning on normal time series data to identify anomaly sequences from reconstruction to solve this error problem. Hence, it seems that combining A.E. and L.S.T.M. can bring about resource-saving and accuracy requirements of the IoT anomaly detection tasks.

4.3.2. Univariate Using Regressive Scheme

Predictive approaches, known as regressive schemes, enable identifying anomalies by comparing predicted value to actual value in time series data. Parametric models such as autoregressive moving average (A.R.M.A.) are popular techniques despite seasonality or mean shift problems in non-stationary datasets. However, these problems can be solved by using enhanced variants of A.R.M.A. such as autoregressive integrated moving average (A.R.I.M.A.) and seasonal A.R.M.A. As another approach to predictive IoT anomaly detection, NN-based predictive models such as M.L.P., R.N.N., L.S.T.M., and others can be applied to capture the dynamics of a time series on complex univariate data [46]. For instance, R.N.N., L.S.T.M., and G.R.U. models can represent the variability in time series data to predict the expected values for time sequences. Recently, attention-based models have been applied to IoT anomaly detection in complex long sequential data. Similar to the non-regressive scheme, sequential models can boost the accuracy of IoT anomaly detection if dimensional reduction algorithms can be used in feature extraction.

4.3.3. Multivariate Using Regressive Scheme

As the additional variables increase data sizes, dimensionality reduction techniques such as P.C.A., A.E., and others can be employed to decrease overall data size. P.C.A. can capture the interdependence of variables for multivariate sources. It reduces the data size by decomposing multivariate data into a reduced set. The linearity and computational complexity of P.C.A. can limit its usage for IoT anomaly detection. A.E. works like P.C.A. and can discover anomalies in multivariate time series data using reconstruction error, the same way as in univariate cases. The promising aspect of A.E. is its low resource usage and its non-linear feature extraction. Similar to predictive and non-predictive models on univariate data, schemes using L.S.T.M., CNN, DBN, and others can also be applied to identifying anomalies in multi-source IoT systems. Specifically, CNN and L.S.T.M. algorithms can be preceded by A.E. for important feature extraction and resource savings. These deep learning schemes can learn spatio-temporal aspects of multivariate IoT data [12].

Clustering mechanisms are another approach to detect anomalies in multivariate data. In addition, graph networks can be used to learn models about variable or sequence relationships where the weakest weight between graph nodes is considered anomalous.

5. Analysis of Machine Learning for IoT Anomaly Detection

Anomaly detection systems have proven their capabilities of defending traditional networks by detecting suspicious behaviours. However, the standalone anomaly detection systems in classical systems do not fit the architecture of distributed IoT networks. In such systems, a single node compromise could damage the entire network. By collecting traffic from various spots, a collaborative anomaly detection framework plays a paramount role in thwarting cyber threats. However, the trust relationship and data sharing form two major challenges [42,51]. In this massive network, insider attacks can be a serious issue.

Furthermore, as most anomaly detection systems apply machine learning, nodes may not be willing to share normal profiles for training or performance optimisation due to privacy issues. The trust problem can be solved by implementing a central server that handles trust computation and data sharing. However, this approach could lead to a single point of failure and security, specifically for the large-scale deployment of IoT devices. Recently, blockchain has attracted much interest in financial sectors for its capability of forming trust among mistrusting entities using contracts and consensus. Blockchain could provide an opportunity to solve the problem of collaborative anomaly detection by providing trust management and a data-sharing platform. In the remainder of this section, we will focus on analysing (1) the collaborative architecture for IoT anomaly detection using blockchain; (2) datasets and algorithms for IoT anomaly detection; and (3) resource requirements of IoT anomaly detection.

5.1. Collaborative Architecture for IoT Anomaly Detection

Blockchain is a decentralised ledger that provides immutability, trustworthiness, authenticity, and accountability mechanisms for the maintained records based on majority consensus. Though it was originally applied to digital currency systems, blockchain can be applied in various fields. With the power of public-key cryptography, strong hash functions, and consensus algorithms, participating nodes in a blockchain can verify the formation of new blocks. A block typically consists of a group of records, timestamp, previous block hash, nonce, and a block's hash. Thus, the change in a record or group of records will be reflected in the next block's previous hash field, which makes it immune to adversarial change [42].

The powerful attributes of blockchain could provide a solid foundation for anomaly detection in distributed networks such as the IoT. IoT devices can collaboratively develop a global anomaly detection model from local models without adversarial attacks using blockchain architecture. As IoT needs mutual trust to share local models in a secure and tamper-proof way, consensus algorithms and decentralised blockchain storage make it challenging for malicious actors to manipulate the network. However, the successful Bitcoin consensus algorithms in financial areas such as proof-of-work require extensive storage and processing capabilities. Etherium has applied proof-of-stake where the participants' stakes determine consensus. It uses smart contracts, and is less computationally intensive. Hyperledger Fabric is another customisable blockchain platform that applies smart contracts in distributed systems rather than cryptocurrencies. As it relies on central service to enable participants to endorse transactions, endorsing participants must agree on the value of a transaction to reflect changes in the local participant ledger. These three popular blockchain systems do not seem to solve resource-constrained IoT devices [51].

Blockchain-based security solutions have been discussed in a mix of traditional and IoT systems [52,53]. In these studies, a resource-rich device was connected to IoT devices, where the device acts as a proxy to connect IoT devices to the blockchain. A similar study was conducted in [54]. The main advantages of these approaches lie in resource savings, but they may also create a central point of failure. In [55], the author's utilised smart contracts to

integrate IoT devices into blockchain for communication integrity and authenticity through the resource requirement issues that may not make it practical. The most promising result has been achieved on distributed and collaborative IoT anomaly detection [51]. The study uses a self-attestation mechanism to establish a dynamic trusted model against which nodes compare to detect anomalous behaviour. The model is cooperatively updated by majority consensus before being distributed to peers.

5.2. Datasets and Algorithms for IoT Anomaly Detection

The lack of labelled realistic datasets has hampered anomaly detection research in the IoT. The existing data suffer from lacking realistic representation for IoT traffic patterns and lack capture of the full range of anomalies that may occur in the IoT. Class imbalance between normal traffic and anomalous patterns also manifests, which makes classification systems inefficient. Most IoT traffic can be represented as normal behaviour while it dynamically changes over time. As contextual information such as time, environment, and neighbour nodes profile rich information to improve anomaly detection in the IoT, it seems that multivariate data plays a significant role. The challenges associated with the absence of truly representative, realistic, and balanced datasets favour an anomaly detection scheme that profiles normal behaviours to detect anomalous points that deviate from the normal data [56]. Table 3 shows the common datasets that have been commonly used in some recent studies in this research area. As can be seen, most datasets are not specific to the IoT system; however, they are still suitable for training and evaluating anomaly-based I.D.S.s because they contain both normal and abnormal data.

Table 3. Common Datasets for Anomaly Detection in the IoT System (Adapted from [1]).

Dataset	Published Year	IoT Specific	Dimensions	Normal Instances	Abnormal Instances
N-BaIoT [57]	2018	Yes	115	555,932	6,545,967
CICIDS 2017 [58]	2017	No	80	2,273,097	557,646
AWID [59]	2015	No	155	530,785	44,858
UNSW-NB15 [60]	2015	No	49	2,218,761	321,283
NLS-KDD [61]	2009	No	43	77,054	71,463
Kyoto [62]	2006	No	24	50,033,015	43,043,255
KDD CUP 1999 [63]	1999	No	43	1,033,372	4,176,086

The initial deployment of the IoT anomaly detection system lacks historical data that specify normal and anomalous points. This absence and the rare nature of anomalies challenge the usage of traditional machine learning schemes. Though several techniques of solving imbalanced data have been proposed, such methods cannot maintain the temporal context of anomalies. In addition, supervised algorithms capture only known anomalies while failing to detect novel attacks. Thus, unsupervised or semi-supervised approaches can be used to solve the limitations of supervised algorithms [54].

While several techniques have been used in IoT anomaly detection, most of the approaches have failed to satisfy the resource and power requirements of IoT devices [54]. Though there is no single best anomaly detection approach, deep learning techniques, specifically A.E. and CNN, have shown promising results in both delivering better resource-saving and accuracy, respectively [64]. While algorithms such as CNN and L.S.T.M. can boost detection accuracy, A.E. can be used to reduce the dimension of data and extract representative features by eliminating noise. Specifically, L.S.T.M. can be applied to dynamic and complex observations within time-series IoT data over a long sequence. Thus, it suggests that these techniques or combinations could be further explored to detect anomalies in the IoT ecosystem [65].

5.3. Resource Requirements of IoT Anomaly Detection

The resource-constrained nature of IoT devices prohibits the deployment of traditional host-based intrusion detection such as anti-malware and anti-virus. As traffic analysis consumes huge computational resources during anomaly detection, incremental approaches such as sliding windows can reduce the processing and storage requirements for IoT devices. It is also critical that the anomaly detection engine of the IoT system should operate in near real-time for reliable detection. This indicates that adaptive techniques help to improve the detection model over time without major retraining. However, offline training may be applied for initial deployment.

6. Conclusions

The IoT environment's massive number, heterogeneity, and resource constraints have hindered cyber-attack prevention and detection capabilities. These characteristics attract monitoring IoT devices at the network level as on-device solutions are not feasible. To this end, anomaly detection is better positioned to protect the IoT network. To protect the system, anomaly detection is considered to be an important tool as it helps identify and alert abnormal activities in the system. Machine learning has been applied for anomaly detection systems in I.T. and IoT systems. However, the applications of anomaly detection systems using machine learning in I.T. systems have been better than the IoT ecosystem due to their resource capabilities and in-perimeter location. Nevertheless, the existing machine learning-based anomaly detection is vulnerable to adversarial attacks. This article has presented a comprehensive survey of anomaly detection using machine learning in the IoT system. The significance of anomaly detection, the challenges when developing anomaly detection systems, and the analysis of the used machine learning algorithms are provided. Finally, it has been recommended that blockchain technology can be applied to mitigate model corruption by adversaries where IoT devices can collaboratively produce a single model using blockchain consensus mechanisms. In the future, we plan to implement a blockchain-based anomaly detection system for protecting high-end IoT devices such as Raspberry Pi. The system can be built on a python-based machine learning platform such as TensorFlow and a blockchain platform such as Hyperledger Fabric, where Raspberry Pi devices act as distributed nodes.

Author Contributions: Conceptualization: A.D. and N.C.; methodology: A.D. and V.-D.N.; formal analysis: V.-D.N.; investigation: V.-D.N.; resources: N.C.; data curation: V.-D.N.; writing—original draft preparation: A.D. and V.-D.N.; writing—review and editing: A.D., V.-D.N., W.H. and N.C.; supervision: N.C.; project administration: N.C. and W.H.; funding acquisition: N.C. and W.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the SmartSat C.R.C., whose activities are funded by the Australian Government's C.R.C. Program.

Conflicts of Interest: The authors declare no conflict of interest in this research.

References

1. 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]
2. Njilla, L.; Pearlstein, L.; Wu, X.; Lutz, A.; Ezekiel, S. Internet of Things Anomaly Detection using Machine Learning. In Proceedings of the 2019 IEEE Applied Imagery Pattern Recognition Workshop (A.I.P.R.), Washington, DC, USA, 15–17 October 2019; pp. 1–6.
3. Cook, A.A.; Mısırlı, G.; Fan, Z. Anomaly Detection for IoT Time-Series Data: A Survey. *IEEE Internet Things J.* **2020**, *7*, 6481–6494. [CrossRef]
4. Cauteruccio, F.; Cinelli, L.; Corradini, E.; Terracina, G.; Ursino, D.; Virgili, L.; Savaglio, C.; Liotta, A.; Fortino, G. A Framework for Anomaly Detection and Classification in Multiple IoT Scenarios. *Future Gener. Comput. Syst.* **2021**, *114*, 322–335. [CrossRef]
5. 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 (S.P.W.), San Francisco, CA, USA, 24 May 2018; pp. 29–35.
6. Hwang, R.H.; Peng, M.C.; Huang, C.W.; Lin, P.C.; Nguyen, V.L. An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection. *IEEE Access* **2020**, *8*, 30387–30399. [CrossRef]

7. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
8. Protogerou, A.; Papadopoulos, S.; Drosou, A.; Tzovaras, D.; Refanidis, I. A Graph Neural Network Method for Distributed Anomaly Detection in IoT. *Evol. Syst.* **2021**, *12*, 19–36. [CrossRef]
9. Cauteruccio, F.; Fortino, G.; Guerrieri, A.; Liotta, A.; Mocanu, D.C.; Perra, C.; Terracina, G.; Torres Vega, M. Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance. *Inf. Fusion* **2019**, *52*, 13–30. [CrossRef]
10. Hasan, M.; Islam, M.M.; Zarif, M.I.I.; Hashem, M. Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches. *Internet Things* **2019**, *7*, 100059. [CrossRef]
11. AL-Hawawreh, M.; 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. [CrossRef]
12. Shukla, R.; Sengupta, S. Scalable and Robust Outlier Detector using Hierarchical Clustering and Long Short-Term Memory (L.S.T.M.) Neural Network for the Internet of Things. *Internet Things* **2020**, *9*, 100167. [CrossRef]
13. Yin, C.; Zhang, S.; Wang, J.; Xiong, N.N. Anomaly Detection Based on Convolutional Recurrent Autoencoder for IoT Time Series. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, 1–11. [CrossRef]
14. Tsogbaatar, E.; Bhuyan, M.H.; Taenaka, Y.; Fall, D.; Gonchigsumlaa, K.; Elmroth, E.; Kadobayashi, Y. SDN-Enabled IoT Anomaly Detection Using Ensemble Learning. I.F.I.P. In *International Conference on Artificial Intelligence Applications and Innovations*; Springer International Publishing: Cham, Switzerland, 2020; pp. 268–280.
15. 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]
16. Farshchi, M.; Weber, I.; Della Corte, R.; Pecchia, A.; Cinque, M.; Schneider, J.G.; Grundy, J. Contextual Anomaly Detection for a Critical Industrial System Based on Logs and Metrics. In Proceedings of the 2018 14th European Dependable Computing Conference (E.D.C.C.), Iasi, Romania, 10–14 September 2018; pp. 140–143.
17. Ferrari, P.; Rinaldi, S.; Sisinni, E.; Colombo, F.; Ghelfi, F.; Maffei, D.; Malara, M. Performance Evaluation of Full-Cloud and Edge-Cloud Architectures for Industrial IoT Anomaly Detection Based on Deep Learning. In Proceedings of the 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0 IoT), Naples, Italy, 4–6 June 2019; pp. 420–425.
18. 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 A.C.M. CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks, Orlando, FL, USA, 9 December 2019; pp. 42–48.
19. Savic, M.; Lukic, M.; Danilovic, D.; Bodroski, Z.; Bajovic, D.; Mezei, I.; Vukobratovic, D.; Skrbic, S.; Jakovetic, D. Deep Learning Anomaly Detection for Cellular IoT With Applications in Smart Logistics. *IEEE Access* **2021**, *9*, 59406–59419. [CrossRef]
20. Ngo, M.V.; Luo, T.; Chaouchi, H.; Quek, T.S. Contextual-Bandit Anomaly Detection for IoT Data in Distributed Hierarchical Edge Computing. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (I.C.D.C.S.), Singapore, 29 November–1 December 2020; pp. 1227–1230.
21. 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 (C.C.W.C.), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310.
22. Utomo, D.; Hsiung, P.A. Anomaly Detection at the IoT Edge using Deep Learning. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW), Yilan, Taiwan, 20–22 May 2019; pp. 1–2.
23. Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. Leveraging Semisupervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. *IEEE Internet Things J.* **2021**, *8*, 144–155. [CrossRef]
24. Han, N.; Gao, S.; Li, J.; Zhang, X.; Guo, J. Anomaly Detection in Health Data Based on Deep Learning. In Proceedings of the 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Guiyang, China, 22–24 August 2018; pp. 188–192.
25. Chalapathy, R.; Toth, E.; Chawla, S. Group Anomaly Detection Using Deep Generative Models. In *Machine Learning and Knowledge Discovery in Databases*; Springer International Publishing: Cham, Switzerland, 2019; pp. 173–189.
26. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.R. DÏoT: A Federated Self-learning Anomaly Detection System for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (I.C.D.C.S.), Dallas, TX, USA, 7–10 July 2019; pp. 756–767.
27. He, Y.; Peng, Y.; Wang, S.; Liu, D.; Leong, P.H.W. A Structured Sparse Subspace Learning Algorithm for Anomaly Detection in UAV Flight Data. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 90–100. [CrossRef]
28. Himeur, Y.; Ghanem, K.; Alsalemi, A.; Bensaali, F.; Amira, A. Artificial Intelligence Based Anomaly Detection of Energy Consumption in Buildings: A Review, Current Trends and New Perspectives. *Appl. Energy* **2021**, *287*, 116601. [CrossRef]
29. Piscitelli, M.S.; Brandi, S.; Capozzoli, A.; Xiao, F. A Data Analytics-Based Tool for The Detection and Diagnosis of Anomalous Daily Energy Patterns in Buildings. *Build. Simul.* **2021**, *14*, 131–147. [CrossRef]
30. Kim, D.; Yang, H.; Chung, M.; Cho, S.; Kim, H.; Kim, M.; Kim, K.; Kim, E. Squeezed Convolutional Variational AutoEncoder for Unsupervised Anomaly Detection in Edge Device Industrial Internet of Things. In Proceedings of the 2018 International Conference on Information and Computer Technologies (I.C.I.C.T.), DeKalb, IL, USA, 23–25 March 2018; pp. 67–71.

31. Kanawaday, A.; Sane, A. Machine Learning for Predictive Maintenance of Industrial Machines Using IoT Sensor Data. In Proceedings of the 2017 8th IEEE International Conference on Software Engineering and Service Science (I.C.S.E.S.S.), Beijing, China, 24–26 November 2017; pp. 87–90.
32. Shah, G.; Tiwari, A. Anomaly Detection in IIoT: A Case Study Using Machine Learning. In Proceedings of the The A.C.M. India Joint International Conference on Data Science and Management of Data. Association for Computing Machinery, Goa, India, 11–13 January 2018; pp. 295–300.
33. Oh, D.Y.; Yun, I.D. Residual Error Based Anomaly Detection Using Auto-Encoder in S.M.D. Machine Sound. *Sensors* **2018**, *18*, 1308. [CrossRef]
34. Giannoni, F.; Mancini, M.; Marinelli, F. Anomaly Detection Models for IoT Time Series Data. *arXiv* **2018**, arXiv:abs/1812.00890.
35. Moghaddass, R.; Wang, J. A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data. *IEEE Trans. Smart Grid* **2018**, *9*, 5820–5830. [CrossRef]
36. Passerini, F.; Tonello, A.M. Smart Grid Monitoring Using Power Line Modems: Anomaly Detection and Localization. *IEEE Trans. Smart Grid* **2019**, *10*, 6178–6186. [CrossRef]
37. Farajollahi, M.; Shahsavari, A.; Mohsenian-Rad, H. Location Identification of Distribution Network Events Using Synchrophasor Data. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017; pp. 1–6.
38. Yip, S.C.; Tan, W.N.; Tan, C.; Gan, M.T.; Wong, K. An Anomaly Detection Framework for Identifying Energy Theft and Defective Meters in Smart Grids. *Int. J. Electr. Power Energy Syst.* **2018**, *101*, 189–203. [CrossRef]
39. El-Wakeel, A.S.; Li, J.; Rahman, M.T.; Noureldin, A.; Hassanein, H.S. Monitoring Road Surface Anomalies Towards Dynamic Road Mapping for Future Smart Cities. In Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, Canada, 14–16 November 2017; pp. 828–832.
40. Kong, X.; Song, X.; Xia, F.; Guo, H.; Wang, J.; Tolba, A. LoTAD: Long-Term Traffic Anomaly Detection Based on Crowdsourced Bus Trajectory Data. *World Wide Web* **2018**, *21*, 825–847. [CrossRef]
41. Bakar, U.A.B.U.A.; Ghayvat, H.; Hasanm, S.F.; Mukhopadhyay, S.C. Activity and Anomaly Detection in Smart Home: A Survey. In *Next Generation Sensors and Systems*; Springer International Publishing: Cham, Switzerland, 2016; pp. 191–220.
42. Alexopoulos, N.; Vasilomanolakis, E.; Ivánkó, N.R.; Mühlhäuser, M. Towards Blockchain-Based Collaborative Intrusion Detection Systems. In *Critical Information Infrastructures Security*; Springer International Publishing: Cham, Switzerland, 2018; pp. 107–118.
43. Hastie, T.; Tibshirani, R.; Friedman, J. *The Elements of Statistical Learning: Data Mining, Inference and Prediction*, 2nd ed.; Springer: New York, NY, USA, 2009.
44. Murphy, K.P. Machine Learning: A Probabilistic Perspective. MIT Press: Cambridge, MA, USA, 2013.
45. Chadha, G.S.; Islam, I.; Schwung, A.; Ding, S.X. Deep Convolutional Clustering-Based Time Series Anomaly Detection. *Sensors* **2021**, *21*, 5488. [CrossRef]
46. Jiang, J.; Han, G.; Liu, L.; Shu, L.; Guizani, M. Outlier Detection Approaches Based on Machine Learning in the Internet-of-Things. *IEEE Wirel. Commun.* **2020**, *27*, 53–59. [CrossRef]
47. Mothukuri, V.; Khare, P.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Srivastava, G. Federated Learning-based Anomaly Detection for IoT Security Attacks. *IEEE Internet Things J. (Early Access)* **2021**. [CrossRef]
48. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 6348–6358. [CrossRef]
49. Lee, H.; Kim, J.; Ahn, S.; Hussain, R.; Cho, S.; Son, J. Digestive neural networks: A novel defense strategy against inference attacks in federated learning. *Comput. Secur.* **2021**, *109*, 102378. [CrossRef]
50. Wang, C.; Chen, J.; Yang, Y.; Ma, X.; Liu, J. Poisoning attacks and countermeasures in intelligent networks: Status quo and prospects. *Digit. Commun. Netw. (Early Access)* **2021**. [CrossRef]
51. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
52. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
53. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized BlockChain for IoT. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
54. Özyılmaz, K.R.; Yurdakul, A. Work-in-Progress: Integrating low-Power IoT Devices to a Blockchain-Based Infrastructure. In Proceedings of the 2017 International Conference on Embedded Software (E.M.S.O.F.T.), Seoul, Korea, 15–20October 2017; pp. 1–2.
55. Huh, S.; Cho, S.; Kim, S. Managing IoT Devices Using Blockchain Platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (I.C.A.C.T.), PyeongChang, Korea, 19–22 February 2017; pp. 464–467.
56. 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. In *Innovative Systems for Intelligent Health Informatics*; Springer International Publishing: Cham, Switzerland, 2021; pp. 659–675.
57. 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]

58. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (I.C.I.S.S.P. 2018), Funchal, Portugal, 22–24 January 2018; pp. 108–116.
59. Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 184–208. [CrossRef]
60. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6.
61. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
62. Malaiya, R.K.; Kwon, D.; Suh, S.C.; Kim, H.; Kim, I.; Kim, J. An Empirical Evaluation of Deep Learning for Network Anomaly Detection. *IEEE Access* **2019**, *7*, 140806–140817. [CrossRef]
63. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P. Cost-based modeling for fraud and intrusion detection: Results from the J.A.M. project. In Proceedings of the DARPA Information Survivability Conference and Exposition, Hilton Head, SC, USA, 25–27 January 2000; Volume 2, pp. 130–144.
64. Kamat, P.; Sugandhi, R. Anomaly Detection for Predictive Maintenance in Industry 4.0-A Survey. In Proceedings of the E3S Web of Conferences, Pune City, India, 18–20 December 2019; p. 02007.
65. Bovenzi, G.; Aceto, G.; Ciuonzo, D.; Persico, V.; Pescapé, A. A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Virtual Event, Taiwan, 7–11 December 2020; pp. 1–7.