# IOT ANOMALY DETECTION METHODS AND APPLICATIONS: A SURVEY \*

#### Ayan Chatterjee

Dept of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden ayan.chatterjee@kau.se

#### Bestoun S. Ahmed

Dept of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden Dept of Computer Science, FEE, Czech Technical University in Prague, Czechia bestoun@kau.se

#### **ABSTRACT**

Ongoing research on anomaly detection for the Internet of Things (IoT) is a rapidly expanding field. This growth necessitates an examination of application trends and current gaps. The vast majority of those publications are in areas such as network and infrastructure security, sensor monitoring, smart home, and smart city applications and are extending into even more sectors. Recent advancements in the field have increased the necessity to study the many IoT anomaly detection applications. This paper begins with a summary of the detection methods and applications, accompanied by a discussion of the categorization of IoT anomaly detection algorithms. We then discuss the current publications to identify distinct application domains, examining papers chosen based on our search criteria. The survey considers 64 papers among recent publications published between January 2019 and July 2021. In recent publications, we observed a shortage of IoT anomaly detection methodologies, for example, when dealing with the integration of systems with various sensors, data and concept drifts, and data augmentation where there is a shortage of Ground Truth data. Finally, we discuss the present such challenges and offer new perspectives where further research is required.

**Keywords** Anomaly detection · Internet of Things · IoT · review · survey · applications.

# 1 Introduction

The Internet of Things (IoT) enables sensors<sup>2</sup> and smart objects to communicate without the direct involvement of human agents, necessitating near real-time processing [1]. Any data analytics performed via IoT requires the development of novel methodologies to work within the limited computational budget. One type of data analysis that looks for unusual states within the system is anomaly detection, also known as outlier detection or event detection. The anomaly detection algorithms are checkpoints for the incoming traffic at various stages, ranging from the IoT network level to the data center. In the latter case, there is a high demand for reliable detection for data cleaning [2] and classification purposes [3].

The significance of anomaly detection is that anomalies in IoT data, which occur sparsely, can yield crucial actionable information in various sectors, including medicine, manufacturing, finance, traffic management, and energy. Anomaly

<sup>\*</sup>Citation: Ayan Chatterjee and Bestoun S. Ahmed. Iot anomaly detection methods and applications: A survey. Internet of Things, 19:100568, 2022. DOI:10.1016/j.iot.2022.100568

<sup>&</sup>lt;sup>2</sup>Throughout this paper, the term 'sensors' refers to sensors or devices attached to an IoT environment, which includes sensors that transmit data to edge, fog, or cloud architectures in an MLOps setting.

detection in IoT, for example, is employed in the betting and gambling sector to detect insider trading by analyzing trade activity patterns [4]. On the other hand, industrial machines use a detection algorithm to ensure production safety [5].

Currently, most anomaly detection methods in the IoT involve significant human engagement and optimizations for local solutions. In theory, an anomaly is simple to comprehend, and a domain expert will spot anomalous data if given enough time. However, there are several difficulties in developing an automated model in an IoT environment. It is challenging and not always possible to define and categorize all types of anomalous data correctly, especially when labeled training data are only partially available/not available. In many fields, the notion of normal behavior is constantly changing and evolving. One such example is a change in household occupancy, which results in a change in electricity demand [6]. Furthermore, data often contain noise, and when the signal-to-noise ratio is low, the magnitude of noise resembles true anomalies. The complexity increases as the number of interconnected systems grows and the variety of input data types.

IoT anomaly detection has a wide range of applications outlined in this paper, some of which are more developed than others (such as network security), and others that have the potential for growth. The literature on the subject of anomaly detection in the IoT is extensive and diverse. However, the discipline is still in its early stages, and the number of articles published on this topic is expanding. Such frequent changes require updated literature. This survey adds to the earlier research and provides a current picture of recent developments and different domains of the IoT anomaly detection application. Additionally, this paper expands on the categorization of anomaly detection algorithms and conducts an extensive keyword trend analysis to demonstrate the year-over-year literature concentration.

The structure of the paper is as follows: Section 2 provides a discussion on the background of anomaly detection algorithm in IoT and related work. The subsequent sections 3 and 4 present the search strategy for this paper and look at recent developments not described in previous reviews to the best of our knowledge. The final section 5 includes new perspectives and concluding remarks.

# 2 Background and related work

# 2.1 Definition and categorization of IoT anomaly detection

An anomaly is a data point that is not associated with the predicted behavior in a modeled system<sup>3</sup> Anomalies are rare events or observations that deviate significantly from conventional behavior or patterns observed in a single data point, a specific context or slice of time (for example, a season or quarter), or the entire dataset. In principle, anomalies result from external factors, such as sensor failure or external attack, and the purpose of a detection algorithm is to identify where an anomaly has occurred and classify/infer the cause. In the binary classification of an anomaly, the approximation model that best fits the expected data behavior is crucial. Furthermore, the complexities of many situations require a distinct detection strategy for each application [7]. Example anomalies are shown in Figure 1.

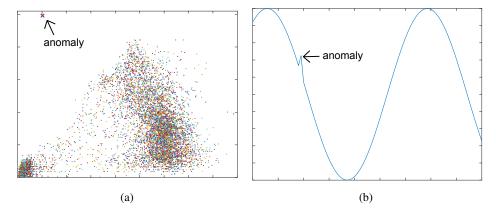


Figure 1: A diagram exhibiting illustrated examples of anomaly.

<sup>&</sup>lt;sup>3</sup>Anomalies in a simple, intuitive explanation are: Given a set of Lego (Lego is a trademark of The Lego Group) pieces, where the building instructions are withheld/unknown from the start, the task of a machine learning model is to generate a set of instructions and construct an object or a character. The remaining pieces that do not fit the trained model are anomalies.

An IoT anomaly detection method is classified into four categories by combining the classifications from previously published articles such as Fahim and Sillitti [8], and Cook et al. [9]. They are categorized based on how they approach the problem, how they are applied, the type of method, and the latency of the algorithm. An illustrative overview of the four categories is displayed in figure 2. This section briefly describes the categorization of anomalies and some of the conventional approaches used in IoT.

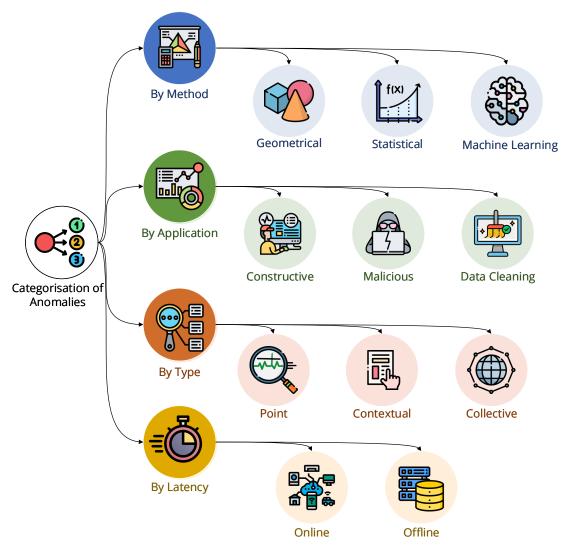


Figure 2: An info-graphic overview of the categorization of anomalies.

i By Method: The approaches are geometrical, statistical, or machine learning. Geometrical methods are based on the assumption that when distance- and density-based strategies represent a given dataset, the expected and anomalous data are separated. In a set of data points, the idea behind isolation or density-based techniques is that anomalies appear in sparse regions. These methods use either a static or a dynamic threshold 't' on the estimated distance 'd' to classify anomalies, which is given as:

$$d = \begin{cases} < t &, & \text{Normal (under threshold)} \\ > t &, & \text{Anomaly (above threshold)} \end{cases}$$
 (1)

Statistical methods such as the minimal volume in [10] try to model normal data using mathematical models and distributions. The minimal volume approach aims to create an n-dimensional simplex around the given data cloud (ground truth), where the objective function is to minimize the volume occupied while maximizing the ground

truth data points. An anomaly is defined as any data that do not fit the simplex. Another is a forecasting approach called exponential smoothing [11]. This technique anticipates the future data point using prior data points and a smoothing parameter. Anomalous data obtained from statistical methods are those that deviate from the established model. Conventional geometrical and statistical methods are backed by a substantial body of research and rely on a thorough understanding of the ground truth. These strategies do not reward many real-world instances in which data models are very time-dependent. Therefore, data-driven machine learning and deep learning solutions are required, which allow for more flexible modifications.

The third subcategory is machine learning and deep learning models, which have increased in publication frequency in recent years. The nature of the data supplied determines the selection of the model [12]. For example, long short-term memory (LSTM) and transformer models prefer sequential data inputs such as audio, video, and time series [13]. On the other hand, the convolutional neural network (CNN) and autoencoder (AE) prefer non-sequential data types, such as image input [14]. The algorithms attempt to distinguish between normal and anomalous behavior by establishing a decision boundary, such as with the support vector machine (SVM) classifier [15] or future forecasting values in streaming data [16] with LSTM networks [17]. Depending on the availability of training labels, these approaches are supervised, semi-supervised, self-supervised, or completely unsupervised [18].

- ii By Application: The three routes of anomaly categorization by an application are constructive, destructive, and data cleaning. Constructive applications are productive or beneficial in nature and provide value to the world, such as monitoring the elderly's daily behavior for fall prevention in [19] using image descriptors and comparing the performance between multilayer perceptron (MLP), k-nearest neighbors (KNN), and SVM classifiers. Other examples include Lu et al.'s work [20] using reinforcement learning for various unmanned aerial vehicle (UAV) applications, including smart farming, and Nguyen et al. [21] using a federated learning approach for smart home applications. Destructive applications are intended to disrupt daily operations to accomplish questionable financial gain, an intention to harm the network and application data flowing through the IoT network, or disrupt critical business practices. These applications negatively impact society; for example, the paper by Alsheikh et al. [22] surveys different IoT cyberattacks and the latest developments in IoT security. Such applications require research into solutions, such as RAPPER [23] and NBaIoT [24] using an AE, for prevention or steps taken before the illicit incident and detection or actions taken after the incident. Finally, data cleaning or data cleansing applications, such as DeepAnT [25] using deep CNN, remove unwanted data spikes and sensor noise from the input signal.
- iii By Anomaly Type: One of the most frequently encountered types is the circumstance-specific type, which is the point, contextual, and collective. An anomaly is a point anomaly if a single data point deviates from the expected behavior. An example is the detection of credit card fraud [26]. A contextual anomaly is an instance that could be considered anomalous in some specific context. This means that comparing multiple perspectives on the same data point does not always result in anomalous behavior. A contextual anomaly is detected when both contextual and behavioral characteristics are considered together. For example, in the case of traffic offences, the anomalies vary depending on the geolocation information [27]. Unlike a point or contextual anomaly, the final type of anomaly, collective anomaly, looks at the entire dataset. An example of a collective anomaly is the use of electrocardiograms to monitor and detect anomalies or problems in the human heart [28].
- iv By Latency: The latency and scalability of a detection algorithm determine whether the method is executed on the fly during the data collection stage or in a later stage of storage. An online algorithm can serially process information, with a single data-point or a window, without having access to the complete input. Conventional online geometrical and statistical approaches include the previously mentioned distance-based, density- and deviation-based, and angle-based techniques. Examples of online methods include the IoT-Keeper by Hafeez et al. [29], which uses fuzzy C-means, and Hedde et al. [30] with an ensemble approach. On the other hand, offline algorithms have access to complete data. They involve relatively computationally expensive and sophisticated algorithms to solve the problem in a reasonable amount of time. However, it is essential to note that in recent years, algorithms such as the paper by Wu et al. [31], which uses LSTM and Gaussian Naive Bayes, and other models mentioned above, complete the model training process offline and deploy the model online.

#### 2.2 Related work and our contribution

A variety of articles on anomaly detection in IoT are published, ranging from expert insight on time-series methods by Cook et al. [32], an introductory summary of the detection methods released between 2000 and 2018 by Fahim and Sillitti [33], an examination of sensor faults and outliers by Gaddam et al. [34], and a comprehensive investigation of the work done in the early twenty-first century by Chandola et al. [35]. The most prevalent forms of surveys are data-specific, application-specific, or method-specific publications. For example, two recent surveys, a paper by Braei and Wagner [36] and another by Mozaffari and Yilmaz [37], examined the use of univariate and multivariate data, respectively. Other examples include the survey by Santos et al. [38] that examines smart city applications on 5G

wide area networks, a review paper on IoT security applications by Ahmad and Alsmadi [39], and anomaly detection using deep learning approaches in a survey by Chalapathy and Chawla [40]. Yassine et al. [41] provide a detailed examination of the methodologies, situations, and computing platforms used in the energy industry.

Despite the fact that this is not a systematic review paper, we did follow many of the techniques, but with some variations. For example, instead of using customized text searches, we developed a bubble chart to visually identify key research areas. Furthermore, based on our search, we found that the developments from 2019 and beyond are insufficient in other review papers. For this reason, our search criteria include papers published between January 2019 and July 2021. Our aim is to discover various IoT anomaly detection applications and report on recent findings. This paper complements the previous literature by:

- i examining publication trends, recent methods, and unique applications in IoT anomaly detection, and
- ii identifying present-day issues and challenges.

# 3 Search strategy

# 3.1 Extraction of keyword trends

In this review, we include only papers published from January 2019 to July 2021. However, to better understand the trends in IoT anomaly detection research, we will extract search keywords from the titles of previous decade publications. We searched Google Scholar using the Publish or Perish tool from [42]. The search criteria were for all article titles in this domain with keywords 'iot' and 'anomaly' published between 2011 and 2020 and excluded duplicate titles. After merging the titles into a string, we extracted the unique keywords and their frequency of occurrence. Subsequently, generic terms such as 'an', 'the', and 'novel' were eliminated from the text. We then sorted the remaining keywords into two categories: (a) methodologies and platforms and (b) applications. Figure 3 shows a bubble chart of publication keywords. Keywords with larger bubbles denote a higher frequency of publications, and smaller bubbles indicate a potential for an increase in contributions. From the figure, we discovered that the methods and platform keywords, which include 'machine learning', 'deep learning', 'distributed', 'edge', 'framework', 'industrial IoT', 'intelligent', 'network', and 'system' all become increasingly relevant for the community. From the applications side, they are 'architecture', 'attacks', 'cyber', 'intrusion detection', 'monitoring', 'security', 'sensor', 'smart devices', and 'wireless'.

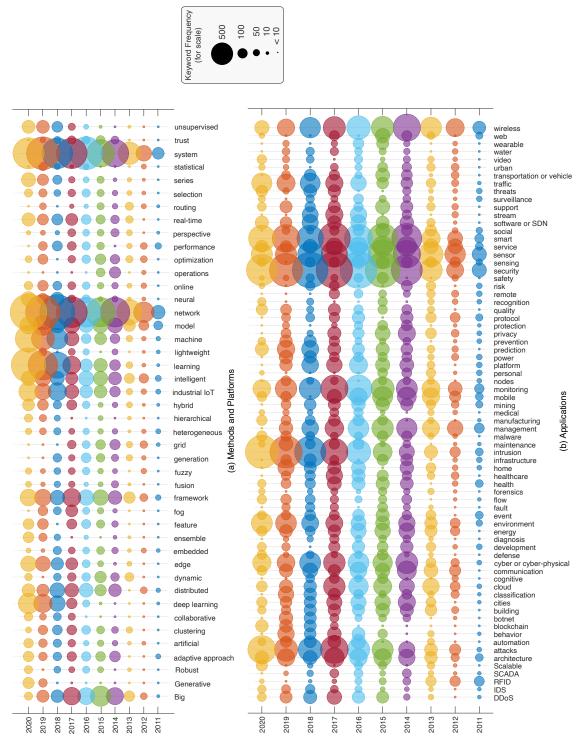


Figure 3: A chart displaying the number of times each keyword is used in article titles. This data is extracted from 8348 unique articles in IoT anomaly detection published between 2011 and 2020.

#### 3.2 Papers' selection criteria

Following the extraction of the keyword trends, we performed a thorough search across established journals and conferences, in the order of the most recently published articles, using the search keywords 'iot', 'anomaly detection', and each of the trending keywords. There were searches in IEEE Xplore, Elsevier ScienceDirect, MDPI, Google Scholar, and arXiv. A total of 2242 articles were collected, which were published between January 2019 and July 2021. Duplicate papers and review publications were then removed using the exclusion keywords 'survey', 'literature review', 'case study', 'reviews', 'systematic review', and 'this review'. The titles of the remaining 1670 manuscripts were rapidly assessed, beginning with the relevance recommendations provided by the search engines mentioned and excluded patents and citation results. At this stage, there were 986 unique articles for further evaluation. Graphing the publishers of the remaining papers in a pie chart in figure 4 reveals that IEEE, Elsevier, Springer, and MDPI account for 76.1 percent of all recent publications.

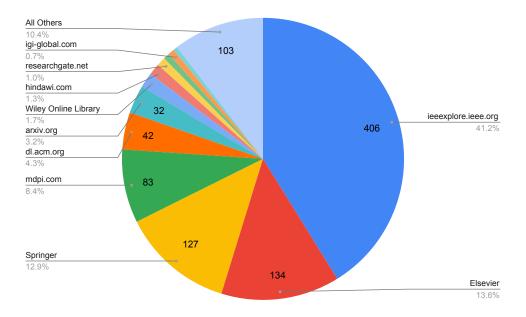


Figure 4: A pie chart illustrating the frequency of articles produced by publisher type between January 2019 and July 2021.

The remaining articles were then filtered with the inclusion keywords 'experiments', 'evaluation,' and 'results.' This allowed us to identify publications that had included experimental results as part of their work. Finally, the abstracts, discussions, and conclusions of the remaining 194 manuscripts were examined to identify papers relevant to the scope of this review. When determining the relevance of the content, the factors taken into consideration are as follows:

- This article made a notable contribution to the field of IoT anomaly detection. Although the search criteria
  specified inclusion and exclusion keywords, publications that were not directly related to this paper's context
  were excluded.
- The publication targeted a unique application domain. Multiple articles in the same application domain, such as botnet attack detection, were narrowed down to the best of our ability, selecting the most recent and higher Google Scholar search rank.

Following the filtering process, we discuss the selected 64 articles published in the previous three years.

## 4 Recent advancements

This section covers the different applications of IoT anomaly detection from the selected papers. Application data and network data are the two main types of data. The data can be streamed in the case of time-series or processed from tabular data. Application data refers to data from IoT sensors processed to serve practical and business applications. Additionally, network telemetry data, such as CPU and memory usage, are monitored for the health of the IoT network.

We found applications that are for individual or residential use and industrial applications. There are health monitoring applications for individuals that use data from wearable devices and smart home applications for residential use-cases. A few examples of industrial applications include monitoring the health of manufacturing equipment, ensuring the quality of data transferred through sensors, and smart city applications such as traffic monitoring. All of these applications require data security, user privacy, and reliability of data transfer. Figure 5 shows the two types of data and their respective applications.

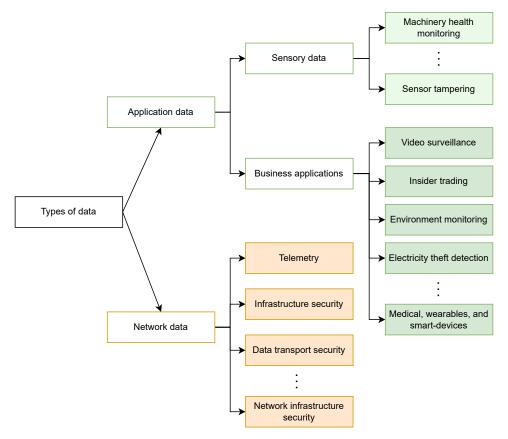


Figure 5: The two types of data (network and application data) and their applications.

On the basis of these data, we combined the different applications into sixteen categories. The categories and the papers are as follows.

#### 4.1 IoT anomaly detection applications with time-series data

The first category is concerned with general time-series or streaming data, which are used in a range of applications. Hierarchical clustering, a non-parametric and lightweight approach, identifies linked sensors and generates clusters. It is possible to utilize a single detection method for all sensors in a cluster. For anomaly detection, the article by Shukla et al. [43] used robust statistical M-estimators paired with the LSTM neural network. Temperature data collected by local weather stations frequently contain missing values and inaccurate readings. The paper by Sobhani et al. [44] shows a substantial relationship between temperature and load. The accuracy of final load projections is improved in the research by eliminating discovered observations from the original input data using local load information. The paper by Ngo et al. [45] demonstrated that using the proposed method in distributed hierarchical edge computing (HEC) systems reduces the detection delay by approximately 71% while the accuracy is maintained. Anomaly detection models for univariate data in the model are built by using AEs. To associate with the three corresponding levels of HEC, the researchers proposed three AE-based models—AE-IoT, AE-Edge, and AECloud. The models have three, five, and seven layers to learn different features for data representation.

The wavelet autoencoder anomaly detection (WAAD) technique [46] initially uses a discrete wavelet transform to produce wavelet transform coefficients by applying a sliding time window to a time-series. The method is applicable on non-stationary and non-periodic univariate time-series data. It then encodes and decodes (reconstructs) these

Application Category	Reference
Time-series data	[43, 44, 45, 46, 47, 48, 49, 50]
Smart city	[51, 52, 53, 54]
Monitoring machinery health	[55, 5]
Robotics and manufacturing	[56, 57, 58]
Detection applications for IoT sensors	[59, 60]
Other industrial or manufacturing	[61, 62, 63, 64]
Surveillance and video	[65, 66, 67]
General-purpose frameworks	[68, 69, 70]
Network and communication frameworks	[71, 72, 73, 74]
User security and privacy frameworks	[75, 76, 77]
Other frameworks	[78, 79]
Network traffic in IoT	[80, 81, 82]
Device and infrastructure security	[83, 21, 84, 85, 86, 87]
Data transport security	[88, 89, 90, 91]
Other security applications	[92, 93, 94, 95, 96, 97, 98, 99, 100]
Miscellaneous IoT applications	[101, 102, 4, 103]

Table 1: A table listing the 64 papers included in this review, as well as their respective application categories.

coefficients using an AE. For every time window, WAAD determines the reconstruction error and obtains to detect anomalous data. To identify local and global anomalies, Chang et al. designed a hierarchical anomaly detection architecture in [47]. High detection accuracy is obtained by combining both edge and cloud servers, respectively. Local anomaly detection focuses on the consistency of the data pattern of individual devices using the Gated Recurrent Unit, which is subsequently sent to the cloud where the global anomaly detection procedure is conducted. The Global IoT anomaly detection looks at how various IoT devices communicate data and uses Conditional Random Fields for detection.

The paper by Yin et al. [48] proposes a new architecture that integrates the convolutional neural network (CNN) and LSTM-based AE. The data from all sensors are collected and delivered to the processing center. Temporal features are extracted using a two-stage sliding window, and higher-level spatial features can be extracted using CNN. The LSTM is then applied to extract high-level temporal characteristics. On the other hand, the C-LSTM model [49] consists of CNN, LSTM-based AE, and deep neural network (DNN) for anomaly detection. This technique applies two-stage sliding window processing to the data for high-level feature extraction. The reconstruction error is used to estimate anomalies in the method.

The HDoutliers algorithm is a powerful unsupervised method for discovering abnormalities in high-dimensional data based on a distributional model that allows outliers to be tagged with a probability. The algorithm tackles the curse of dimensionality, scalability, categorical variables, and non-normal distributions. To overcome the shortcomings of HDoutliers, the paper by Talagala et al. [50] offers an improved technique for anomaly detection that uses higher-dimensional data, called the stray algorithm.

# 4.2 Monitoring the health of machinery

In contrast to the previous category, which looked at general time-series data, this category monitors the application data flowing from IoT sensors attached to industrial machinery and seeks machine faults. The proposed Mahalanobis–Taguchi method [55] is used to detect changes in the mechanical condition of the facilities. This technique can be used to keep an eye on the level of fatigue in logistic systems. Researchers in the paper have studied ways to detect damage to rotating equipment, such as bearings and gearboxes. By using the Mahalanobis distance, the method can calculate the feature vectors of the anomaly vibration data. A condition-based maintenance (CBM) approach can minimize scheduled and unscheduled breakdowns, as well as losses in production. CBM's primary purpose is to spot anomalies and anomalies that don't conform to any explicit laws and monitor those anomalies while they are still in progress. The Narrow Band Internet of Things (NB-IoT) technique is used in Li et al.'s work [5] to

design a condition monitoring system for machinery equipment. In this approach, sensor data is sent to a server that then locates the cause of the anomalies in time and decides how much damage has been done. It uses wavelet packet decomposition to extract the features of the vibration signal.

#### 4.3 Robotics or manufacturing applications

The third category inputs application data for anomaly detection in robotics and manufacturing. In the paper by Chen et al. [56] a real-time anomaly detection system for industrial robots was created using a variational AE (VAE). The method was tested by injecting faults into the robot and observing how the robot resolved them. To cope with multiple time-series data, the proposed model can detect anomalies spatially and temporally. Another novel method to detect anomalies in the manufacturing process in [57] implements an unsupervised feature reduction method based on mutual information (MI) and conditional mutual information (CMI). A clustering model based on density peak (DP)-weighted fuzzy C-means (WFCM) is proposed to detect anomalies. An anomaly detection method for gearbox oil temperature utilizing SCADA data is proposed in [58]. In the process, domain knowledge such as wind speed, power, low/high-speed shaft temperature, and intake oil temperature, respectively, Pearson correlation and Spearman rank correlation are used to measure the association between gearbox oil temperature and other directly related factors or indirectly related.

#### 4.4 Detection applications for IoT sensors

The IoT-CAD method [59] proposes a context-aware adaptive data-driven monitoring system for IoT systems that can detect changes in sensor signals caused by an unexpected event in the environment. The process considers the correlation between the levels of oxygen, ammonia, and nitrate in the water tanks. The model is made to be adaptable and able to self-update. By monitoring changes in temperature and pressure, the model can detect anomalous rises in nitrate levels. Alternatively, Cui et al.'s approach [60] uses Spatio-temporal correlation to detect anomalies in IoT sensors. The method has two stages: (i) the anomaly source identification stage is completed by a fuzzy logic system based on Spatio-temporal correlation, and (ii) the anomaly detection stage using a composite distance metric and sensor clustering. The approach exploits the temporal sequence to get the historical spatial correlation degree, i.e., historical feature parameters.

#### 4.5 Other industrial or manufacturing applications

Other approaches include merging edge devices' electricity data with weather data allows [61] method to create a sparse anomaly perception model. By following this method, anomalous data can be labeled quickly and efficiently. Navigation and planning tasks are particularly vulnerable to driving errors in autonomous vehicles. The safety and security of connected autonomous vehicles' passengers are essential for the development of autonomous vehicles. The method by Zekry et al. [62] proposes an IoT sensor-assisted convolutional long short-term memory (LSTM) model for connected vehicles for anomaly detection. The method by Wang et al. [63] targets log anomalies in large-scale IoT systems. Using a natural language processing approach, the researchers extracted the relevance between words and vectorized them. The method trains supervised models (Random Forests, Naive Bayes, and Neural Networks) to detect anomalies and cites a 30x reduction in computational time. Dang et al. [64] proposes a novel monotone split and Conquer (MSC) strategy to detect short and long forms of anomalies. The MSC model has an offline training phase and an online detection phase. The method extracts sub-trends from the data and uses the multi-scale PCA algorithm to generate a normal data profile.

#### 4.6 Smart-city IoT applications

Smart-city and urban applications include the paper by Xu et al. [52] proposed an integrated IoT anomaly detection method, dubbed I-LSTM, presented based on the concept drift adaptive and deep learning methods to detect anomalies in smart-city data. The effectiveness of I-LSTM is with a smooth activation function for multi-classification anomaly detection, which can obtain the specific anomaly classification to improve the integrated quality of service of a smart home. To differentiate valid and noisy Photoplethysmography (PPG) signals collected from wearable devices, the quality assessment lightweight PPG method [51] employs the Mahalanobis distance measure. The approach is non-invasive and is suitable for monitoring vital indicators such as heart rate, breathing rate, and blood oxygen saturation without subjecting the patient to procedures that could become unnecessary.

Smart cameras and temperature-meters tied to an edge gateway at quick service restaurants predict demand, creating timely alerts and intelligent decisions for proactive waste management. The approach by Aytaç and Korçak [53] is one such application to detect sensor defects, monitor security attacks, and detect increased foot traffic in restaurants in the

edge environment of IoT. The stored data are first broken down into separate groups with the K-means clustering or Lloyd's method. Following the implementation of the clustering method, the experiment is executed to determine the correctness of the clustering results. Then anomalies are discovered based on the Bhattacharyya distances. Another application is in the medical sector to protect the safety and privacy of the patient's personal and medical data in a smart city, the paper by Tripathi et al. [54] proposed the Smart Medical System (SMS) method. Classical healthcare systems were shown to have notable shortcomings and their incompatibility with smart city systems. The proposed framework suggests safe, rapid, reliable, and transparent city-wide connectivity based on IoT, MEC, and blockchain consensus processes. Because the data need to travel only a small distance between the sensor and the edge nodes, it is faster, uses less energy, and is more cost-effective with fewer data losses.

## 4.7 Surveillance and video IoT applications

This category includes IoT anomaly detection algorithms that make use of application data from cameras and remote sensing sensors. Inadequate monitoring of electrical equipment can result in massive economic losses and societal impacts. Hou et al. [65] proposed an image anomaly detection method for IoT equipment based on deep learning for both personnel identification and fire smoke detection to address the problem. The researchers used the approach to monitor the safety of the power equipment's working environment and people identification, and fire smoke detection. The main contribution includes introducing color features, texture features, and shape irregularities to increase the recognition rate. Furthermore, based on deep convolutional neural networks, the algorithm detects fire smoke.

Another is a surveillance system developed for hostile environments for the Tunisian army, dubbed Read-IoT [66]. The project's primary goal is to design a system for monitoring security threats that is both dependable and complete. The proposed system, READ-IoT, applies to IoT networks of heterogeneous objects such as cameras, sensors, and drones. The READ-IoT framework responds to real-time constraints and helps to reduce system downtime for cloud or fog computing. Threat detection is handled automatically and appropriate responses are executed. The approach requires cascaded activation of detection components. Data from each subsystem (anomaly detection system and event detection system) are funneled into a centralized source for effective decisions in the field.

The third is a proposed framework by Ullah et al. [67] that reduces the amount of time required to identify abnormal occurrences in surveillance networks. The proposed system incorporates bi-directional LSTM with CNN characteristics to identify and classify anomalous incidents in the real world. In this pipeline, CNN features are collected from successive frames, and then a new multi-layer LSTM is used to distinguish the normal and abnormal. The deep features and multi-layer BD-LSTM provide flexible, high-level training and validation data to real-world surveillance networks. This framework might be used by law enforcement at airports and hospitals, for example.

## 4.8 General-purpose frameworks

With network and application data, the following four categories outline the recent frameworks and their applications. General-purpose frameworks include the robust anomaly detection framework (RAD Framework) [68] developed for less reliable data. The framework utilizes SVM, KNN, random forest, and nearest centroid classifiers. The authors claim to achieve an accuracy of up to 98% for attacks on IoT devices and cluster failure prediction, and comment that the accuracy reduction is due to general reduction in clean data and noise pollution. For industrial IoT applications, Wang and Ahn [69] found that monitoring current power consumption is not sufficient to meet the second-by-second balance between power consumption and generation. To approach the problem, the article proposes a hybrid one-step-ahead load predictor (OSA-LP) and a rule-engine-based load anomaly detector (RE-AD), a framework that could detect anomalies in residential power usage in real-time. Koduru et al. [70] proposed another framework that creates a pipeline for a weather monitoring system. The framework uses a few sensors to provide information on any unexpected weather changes, and the findings are displayed on a smartphone.

# 4.9 Frameworks for network applications

The frameworks that make use of network data fall into the following group. From a network, network security, and communication standpoint, AnoML-IoT [71] is a data science pipeline that integrates several wireless communication protocols, anomaly detection algorithms, and deployment to edge, fog, and cloud platforms with little user input. The pipeline covers four major phases: data intake, model training, model deployment, inference, and maintenance. The DeL-IoT framework [72] for IoT anomaly identification and prediction uses a deep ensemble learning technique to identify anomalies. The framework detects IoT abnormalities by dynamically observing packet and flow level traffic instances that pass through SDN switches and system metrics. In the scalable framework by Mirsky et al. [73], a distributed and collaborative anomaly detection algorithm is created using the concept of blockchain. The method uses a probabilistic model called a Markov chain (MC) to simulate sequences efficiently. An et al. [74] proposed

a unique anomaly detection framework for the IoT, which is capable of relieving network congestion and central processing units (CPUs) from the computing pressures of centralized servers while unlocking the potential of edge intelligence (EI) in the IoT. The framework uses clustering and classification algorithms sequentially.

# 4.10 User security and privacy preserving frameworks

Frameworks that incorporate user security and privacy, like the paper by Liu et al. [75] proposes a framework for on-device personal data processing and handles user data locally. An attention mechanism-based neural network is used in this on-device federated learning framework. As part of this system, each edge device utilizes the local dataset to train the global model supplied by the cloud aggregator and then transfers the gradients back to the cloud aggregator until convergence. Decentralized Industrial IoT devices might make use of global anomaly detection algorithms in this way. The MIoT framework [76] provides a multi-dimensional view of the anomalies and the accompanying issues. The model considers two kinds of content anomalies: tight content anomalies, in which the complete set of reference keywords must be included in the related transactions, and loose content anomalies, in which at least one of the reference keywords must be present. Another paper [77] proposes a more efficient approach for detecting malicious behavior in SDN and edge computing networks. The method helps verify the trustworthiness of edge devices for data forwarding while maintaining data secrecy throughout data transmission and exchange.

#### 4.11 Other frameworks

Other frameworks like the paper by Li et al. [78] use sensor processing, smart meter readings, and a blockchain to detect anomalies in electricity use accurately and on time. Using the system, factories and residents can be warned to reduce electricity use. Anomaly detection in IoT data is performed using a service selection framework by Yang et al. [79]. The model utilizes a rapid classification algorithm, which is an XGBoost implementation that is taught to recognize distinct stream data patterns and allow for the training of new decision models.

#### 4.12 Network traffic in IoT

Network traffic analysis (NTA) is a specialized topic within network traffic prediction. In ad hoc IoT networks, such as when using ML-based NTM methods, training is time-consuming, and unexpected occurrences or departures are often missed. TONTA [80], a suggested online anomaly and trend change detection technique, is used by all nodes responsible for data forwarding. Although TONTA identifies the predominant trend changes, some events can cause jitters, e.g., performance of communication protocols and network congestion, to name a few. The Green Energy Efficient Routing with Deep Learning Based Anomaly Detection (GEERDLAD) model [81] provides an effective use of energy to help increase the network span. Anomaly detection in the IoT communication networks is carried out in the algorithm through the recurrent neural network-long short term memory (RNN-LSTM) model. Furthermore, the paper by Shen et al. [82] proposes a privacy-preserving SVM training strategy, called secure SVM. The method uses encrypted IoT data, in which data providers encrypt their data locally using their private keys and then record the encrypted data on the blockchain through specially structured transactions.

## 4.13 Security applications for IoT devices and infrastructure

The IoT anomaly detection community is focused primarily on security applications. Because of the large number of publications in this sector, it is not possible to cover all of them; nonetheless, we have categorized security applications into three categories - (i) devices and infrastructure, (ii) data transport, and (iii) miscellaneous applications. This section discusses the first of the three categories, devices and infrastructure, which use a combination of streaming application data and network data to identify security anomalies affecting connected hardware devices.

In Pathak et al.'s paper [83], the researchers used the isolation forest approach to detect sensor tampering. Sensor tampering is detected using network traffic data and is applicable in an industrial and office environment. The algorithm takes packet length, packet-length-daily count, and hash value as input, along with the Silhouette coefficient metric for evaluating the goodness of a clustering technique. A distributed and self-learning approach, DIOT is an autonomous, self-propelling system that aims to find compromised IoT devices. It automates device-specific communication profiles built on through device-type-specific communication profiles with no human intervention or labeled data, which are used to detect anomalies in devices' behavior. The paper by Nguyen et al. [21] has a dedicated model for each device type for different IoT devices with different behaviors. To improve global model accuracy, the DIOT approach by Yahyaoui et al. [84] has an ensembler part aggregating changes from multiple sources and then optimizes the model's accuracy. Instead of having two gates for each memory cell, they only use two gates in total, the Reset gate and Update gate. The approach is for AI-powered anomaly detection on IoT networks, utilizing federated learning. The system has a Virtual Instance, a local deep learning model, and an ensembler component with a high-level architecture.

The design of a distributed anomaly-detection system involves implementing a graph neural network (GNN) method [85]. This system is designed to thoroughly monitor all of the network's infrastructure. GNN monitoring is performed to monitor nodes and devices connected to those nodes using the underlying graph structure. To protect private data from home devices, Venkatraman et al. [86] used a Probabilistic Timed Automaton (PTA) to model the activities of smart devices, keeping intruders from stealing confidential data. Furthermore, Said et al. [87] use the support vector machine (SVM) classifier to help preserve data accuracy while avoiding sending false alerts to hospital infrastructure. Body temperature and heartbeat data are among the applications.

# 4.14 Security application for IoT data transport

The second category of IoT anomaly detection for security applications is data transport. The methods used in this application provide secure and uncompromised transit of application data through the network and identify malleable attacks such as man-in-the-middle and trojans. Niraja et al. [88] propose an adaptive hybrid strategy for near-real-time detection of IoT cyberattacks to improve IoT security. It is based on the integration of deep AE and feature extraction. During the process, it performs encoding and decoding to have the data compressed and reconstructed, respectively, to detect anomalies or attack traffic generated by compromised IoT devices. Fouad et al. [89] propose a technique to detect attacks, trojans, and malfunctions. It is beneficial for the detection of attacks with low training samples. Hidden Markov models (HMM) are used in all aspects of the model, and power signature analysis is used to detect anomalies. Developing new methodologies to discover compromised IoT devices is imperative as there will be significant impacts if IoT botnet attacks are left unmanaged. The proposed method by Shorman et al. [90] makes the main contribution in botnet attack detection using the Grey Wolf Optimization algorithm. The Song et al.'s technique [91] uses a deep packet inspection (DPI) approach and is based on the Three Sigma Rule and Hurst parameter. Using DPI-based solutions, network operators can provide a detailed view of network usage, identify heavy users, and respond quickly to network traffic. This is useful for finding and preventing network abnormalities that lead to increased use of router resources.

#### 4.15 Other security applications

The third security category is miscellaneous and covers applications that indirectly affect IoT sensors, infrastructure, application, network, or ML models. For example, in MLOps, where continuous delivery and execution of ML software in containers such as Docker containers running in Kubernetes are required, network data are utilized to evaluate whether an unexpected container shutdown is from a security attack. In a distributed denial of service (DDoS) attack, the network is bottlenecked by incoming handshaking requests.

The article by Vu et al. [92] presents a learning approach that inherits the strength of supervised learning approaches to identify known threats to VAEs. VAEs learn to map incoming data into a single area in its bottleneck layer using the standard Gaussian shape. The experimental findings indicate that the proposed models can map nonlinear separable normal and attack data in their original space to linear and isolated data in their latent feature space. Wang's paper [97] suggests a network-monitoring algorithm built around a cluster-based routing method. Cyber-attacks like DDoS attacks are detected with this method. The credibility level is evaluated, and anomalous activity is monitored with a trusted function module in this approach.

The edge network, including routers and switches in locations such as the airport and gateway, is safeguarded with a proposed ensemble one-class statistical learning model by Moustafa et al. [93] that implements Gaussian Mixture-based Correntropy. The proposed system aims to identify zero-day attacks and also attempts to develop a legitimate profile for new data flows as they occur. Data mining methodologies that include clustering and rule discovery, statical approaches, and machine learning approaches have been the core hierarchy for anomaly detection-based intrusion detection systems. The proposed system called IoT-based Intrusion Detection and Classification System using Convolutional Neural Network (IoT-IDCS-CNN) [94] has three subsystems: a feature engineering subsystem, a feature learning subsystem, and a traffic classification subsystem. The paper by Dymora and Mazurek [95] used fractal analysis to identify potential security problems in a network. Based on the findings of the paper, it appears that it would be possible to detect both short-term attacks and more intense ones. Basati and Faghih's approach [96] proposes a real-time network intrusion detection system that employs two AEs in parallel to monitor the network and a feature reduction deep AE to identify the most distinct features.

A stacked ensemble meta-learning (SEM) model [98] is proposed to boost the effectiveness of the base machine learning model for IoT device anomaly detection. This design builds a higher-level prediction model that encompasses the predictions of base classifiers that have low accuracy. To have a high-level prediction, the approach utilizes a meta-learning prediction approach. The goal of Bhatia and Sangwan's paper [99] is to make debugging and explaining

easier using fewer features. The approach uses an ensemble feature selection to eliminate the bias of individual feature selection methods during the ensemble and identifies the optimal subset with non-redundant and relevant features.

Furthermore, Kurt et al. [100] propose extracting useful univariate summary statistics from observed high-dimensional data and performing anomaly detection in a single-dimensional space. Suppose that the observed data have low intrinsic dimensionality. In that case, the method learns a submanifold in which the nominal data are embedded and determines whether the sequentially acquired data persistently deviate from the nominal submanifold. In the general case, Geometric Entropy Minimization is used to learn an acceptance region for nominal data and evaluate whether the sequentially observed data consistently fall outside the acceptance region.

#### 4.16 Miscellaneous IoT applications

IoT anomaly detection is still a developing field, with some applications receiving fewer publications than others. The last category, miscellaneous, includes applications in their early stages of development. This includes the paper by Liu et al. [102], which discussed the data acquired by several mining sensors and the requirement for real-time tracking of safety warnings. Construction safety monitoring is performed to look for inconsistencies in the data gathered by the sensors. In this approach, anomaly detection tasks are separated from the sensor and sink nodes and assigned to distinct nodes in the network. Then, algorithms are built for each kind of node, allowing for more processing flexibility. In noisy environments, the ITrust model [101] can detect anomalous or faulty nodes more effectively than current trust models. This model is primarily intended for underwater acoustic sensor networks. The ITrust, which contains four trust metrics (communication trust, data trust, energy trust, and environmental trust), is built on the isolation forest algorithm. The paper by Min et al. [4] proposes a framework for Mobile Horse Racing Betting (MHRB) relying on IoT sensors, devices, and applications. The framework considers recurrent neural network (RNN), long short-term memory (LSTM), and statistical methods to discover insider trading. Furthermore, as IoT devices collect an enormous amount of communication records, the data rapidly. In Cheng et al.'s paper [103], a semi-supervised model was developed to identify anomalies in such scenarios. The method uses a stacking approach, which is an effective way to evaluate data without a label. It is used to discover records with uncertain data and eliminate them.

The section concludes with a table in 2 of fifteen articles having a distinct application domain and with the highest citation count from 2019 until July 2021 (five for each year).

Paper	Application	Publisher	Cites
[104]	Botnet attack detection	Elsevier	253
[105]	Blockchain-based encrypted IoT data	IEEE	164
[21]	Federated approach for smart home	IEEE	131
[106]	Flow detection in software-defined networks	IEEE	112
[107]	Attacks in cyber manufacturing systems	Springer	110

(a) 2019

Paper	Application	Publisher	Cites
[108]	Approach to intrusion detection	Springer	73
[90]	IoT botnet detection	Springer	56
[109]	Industrial big data applications	IEEE	52
[110]	Gray hole attack detection	Springer	48
[111]	Framework to determine trustworthiness	IEEE	44

(b) 2020

Paper	Application	Publisher	Cites
[112]	IoT generated DDOS traffic detection	Springer	29
[67]	Detection in surveillance networks	Springer	22
[113]	Blockchain-based systems intrusion detection	IEEE	22
[114]	Cybersecure IoT and 5G infrastructure	Elsevier	16
[115]	Multiple IoT scenarios in a smart city	Elsevier	15

(c) 2021

Table 2: Fifteen papers with the highest citation count (as of 5th of August 2021) are listed on this table (five for each year). They are grouped by year and has a unique application domain.

# 5 Conclusions and new perspectives

The frequency of publication in IoT anomaly detection shows that the field is still in its early stages. Anomaly detection algorithms are classified into four categories, which are briefly summarized in this review. It also lists the most commonly used keywords and applications and identifies application domains that require further research. Lastly, based on our search criteria, this review discusses 64 novel papers published between January 2019 and July 2021, each with a distinct application domain. As per our current knowledge, there is no single best generic algorithm for the problem but rather a number of methods specific to a particular application. In this section, we attempt to narrow down a large number of possibilities to some of the most significant issues facing the field today. The new perspectives are beneficial for univariate, multivariate, as well as for dealing with high-dimensional data. They are:

- Unsupervised, semi-supervised, and self-supervised approach:
  Obtaining labeled training data is time-consuming, expensive, and not always possible. Furthermore, the labeled data may not accurately represent all anomalous data present in the dataset. There may also be an imbalance between the types of anomalous data present for training and testing. As a result, a self-supervised, semi-supervised, and unsupervised algorithm, especially as an online approach, that can achieve detection accuracy comparable to that of supervised approaches is desirable.
- Detection for multi-representation data traffic:

  The representation data from one or more types of sensors may be sent over the same data pipeline. One such use is external building profiling in an urban environment [116], which involves the integration of RGB cameras with sensors such as hyperspectral, LiDAR, and thermal, among others. A detection algorithm capable of handling volumes of multi-representation data flow at scale and with great precision and recall is viable for these types of applications.

- Drift adaptation:
  - A factor in the accuracy of a trained model is the distribution and quality of the data available during the training process. Over time, when the distribution of the incoming traffic differs from the distribution of the training data, there is a data drift [117]. In such cases, it is common for the model to require re-training. It is preferable for an anomaly detection model to take a more proactive strategy to adapt to incoming data or concept drifts.
- Learning and testing from augmented data:

  In order to train a classification algorithm, it is necessary to have enough accurate and reliable data. This is especially true for the binary classification of anomaly detection. However, when there are insufficient data available for one or more classes, statistical and machine learning-based data augmentation methods such as the generative adversarial network (GAN) generate more training samples [118]. A robust detection technique that utilizes data augmentation in model training and software testing is required for applications with insufficient data.

# Acknowledgments

This work has been funded by the Knowledge Foundation of Sweden (KKS) through the Synergy Project AIDA - A Holistic AI-driven Networking and Processing Framework for Industrial IoT (Rek:20200067).

# References

- [1] Hanan Elazhary. Internet of things (iot), mobile cloud, cloudlet, mobile iot, iot cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. *Journal of Network and Computer Applications*, 128:105–140, 2019.
- [2] Ane Blázquez-García, Angel Conde, Usue Mori, and Jose A. Lozano. A review on outlier/anomaly detection in time series data. *ACM Comput. Surv.*, 54(3), April 2021.
- [3] Ibrahim Arif and Nevena Ackovska. *IoT Aided Smart Home Architecture for Anomaly Detection*, pages 1–19. Springer International Publishing, Cham, 2021.
- [4] Moohong Min, Jemin Justin Lee, Hyunbeom Park, and Kyungho Lee. Detecting anomalous transactions via an iot based application: A machine learning approach for horse racing betting. *Sensors*, 21(6), 2021.
- [5] Chenyang Li, Lingfei Mo, Hanru Tang, and Ruqiang Yan. Lifelong condition monitoring based on nb-iot for anomaly detection of machinery equipment. *Procedia Manufacturing*, 49:144–149, 2020. Proceedings of the 8th International Conference on Through-Life Engineering Services – TESConf 2019.
- [6] Jun-Yeol Ryu, Dae-Wook Kim, and Man-Keun Kim. Household differentiation and residential electricity demand in korea. *Energy Economics*, 95:105090, 2021.
- [7] Xin-Xue Lin, En-Hau Yeh, and Phone Lin. *Anomaly Detection for IoT Systems*, pages 18–20. Springer International Publishing, Cham, 2020.
- [8] Muhammad Fahim and Alberto Sillitti. Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. *IEEE Access*, 7:81664–81681, 2019.
- [9] Andrew A. Cook, Göksel Mısırlı, and Zhong Fan. Anomaly detection for iot time-series data: A survey. *IEEE Internet of Things Journal*, 7(7):6481–6494, 2020.
- [10] Colin O'Reilly, Alexander Gluhak, and Muhammad Ali Imran. Distributed anomaly detection using minimum volume elliptical principal component analysis. *IEEE Transactions on Knowledge and Data Engineering*, 28(9):2320–2333, 2016.
- [11] Sachit Mahajan, Ling-Jyh Chen, and Tzu-Chieh Tsai. Short-term pm2.5 forecasting using exponential smoothing method: A comparative analysis. *Sensors*, 18(10), 2018.
- [12] Adam S. Charles. Interpreting deep learning: The machine learning rorschach test?, 2018.
- [13] Zekai Chen, Dingshuo Chen, Xiao Zhang, Zixuan Yuan, and Xiuzhen Cheng. Learning graph structures with transformer for multivariate time series anomaly detection in iot. *IEEE Internet of Things Journal*, pages 1–1, 2021.
- [14] Arijit Ukil, Soma Bandyoapdhyay, Chetanya Puri, and Arpan Pal. Iot healthcare analytics: The importance of anomaly detection. In 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), pages 994–997, 2016.

- [15] Kun Yang, Samory Kpotufe, and Nick Feamster. An efficient one-class svm for anomaly detection in the internet of things, 2021.
- [16] Murray Dunne, Giovani Gracioli, and Sebastian Fischmeister. A comparison of data streaming frameworks for anomaly detection in embedded systems. In *Proceedings of the 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), Orlando, FL, USA*, 2018.
- [17] Di Wu, Zhongkai Jiang, Xiaofeng Xie, Xuetao Wei, Weiren Yu, and Renfa Li. Lstm learning with bayesian and gaussian processing for anomaly detection in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(8):5244–5253, 2020.
- [18] Muhammad Fahim and Alberto Sillitti. Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. *IEEE Access*, 7:81664–81681, 2019.
- [19] Yves M. Galvão, Vinicius A. Albuquerque, Bruno J. T. Fernandes, and Mêuser J. S. Valença. Anomaly detection in smart houses: Monitoring elderly daily behavior for fall detecting. In 2017 IEEE Latin American Conference on Computational Intelligence (LA-CCI), pages 1–6, 2017.
- [20] Huimin Lu, Yujie Li, Shenglin Mu, Dong Wang, Hyoungseop Kim, and Seiichi Serikawa. Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. *IEEE Internet of Things Journal*, 5(4):2315–2322, 2018.
- [21] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. DÏot: A federated self-learning anomaly detection system for iot. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pages 756–767, 2019.
- [22] Mohammed Alsheikh, Liam Konieczny, Michael Prater, Gabe Smith, and Suleyman Uludag. State and trends of iot security: Unequivocal appeal to cybercriminals, onerous to defenders. *IEEE Consumer Electronics Magazine*, pages 1–1, 2021.
- [23] Manaar Alam, Sayan Sinha, Sarani Bhattacharya, Swastika Dutta, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. Rapper: Ransomware prevention via performance counters, 2020.
- [24] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, 2018.
- [25] Mohsin Munir, Shoaib Ahmed Siddiqui, Andreas Dengel, and Sheraz Ahmed. Deepant: A deep learning approach for unsupervised anomaly detection in time series. *IEEE Access*, 7:1991–2005, 2019.
- [26] Panigrahi Srikanth. An efficient approach for clustering and classification for fraud detection using bankruptcy data in iot environment. *International Journal of Information Technology*, pages 1–7, 2021.
- [27] Shreya Asoba, Shreya Supekar, Tushar Tonde, and Juned A. Siddiqui. Advanced traffic violation control and penalty system using iot and image processing techniques. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pages 554–558, 2020.
- [28] Hongzu Li and Pierre Boulanger. A survey of heart anomaly detection using ambulatory electrocardiogram (ecg). *Sensors*, 20(5), 2020.
- [29] Ibbad Hafeez, Markku Antikainen, Aaron Yi Ding, and Sasu Tarkoma. Iot-keeper: Detecting malicious iot network activity using online traffic analysis at the edge. *IEEE Transactions on Network and Service Management*, 17(1):45–59, 2020.
- [30] Hedde H.W.J. Bosman, Giovanni Iacca, Arturo Tejada, Heinrich J. Wörtche, and Antonio Liotta. Ensembles of incremental learners to detect anomalies in ad hoc sensor networks. *Ad Hoc Networks*, 35:14–36, 2015. Special Issue on Big Data Inspired Data Sensing, Processing and Networking Technologies.
- [31] Di Wu, Zhongkai Jiang, Xiaofeng Xie, Xuetao Wei, Weiren Yu, and Renfa Li. Lstm learning with bayesian and gaussian processing for anomaly detection in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(8):5244–5253, 2020.
- [32] Andrew A. Cook, Göksel Mısırlı, and Zhong Fan. Anomaly detection for iot time-series data: A survey. *IEEE Internet of Things Journal*, 7(7):6481–6494, 2020.
- [33] Muhammad Fahim and Alberto Sillitti. Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. *IEEE Access*, 7:81664–81681, 2019.
- [34] Anuroop Gaddam, Tim Wilkin, and Maia Angelova. Anomaly detection models for detecting sensor faults and outliers in the iot a survey. In 2019 13th International Conference on Sensing Technology (ICST), pages 1–6, 2019.

- [35] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM Comput. Surv.*, 41(3), July 2009.
- [36] Mohammad Braei and Sebastian Wagner. Anomaly detection in univariate time-series: A survey on the state-of-the-art, 2020.
- [37] Mahsa Mozaffari and Yasin Yilmaz. Online anomaly detection in multivariate settings. In 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), pages 1–6, 2019.
- [38] José Santos, Philip Leroux, Tim Wauters, Bruno Volckaert, and Filip De Turck. Anomaly detection for smart city applications over 5g low power wide area networks. In *NOMS 2018 2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–9, 2018.
- [39] Rasheed Ahmad and Izzat Alsmadi. Machine learning approaches to iot security: A systematic literature review. *Internet of Things*, 14:100365, 2021.
- [40] Raghavendra Chalapathy and Sanjay Chawla. Deep learning for anomaly detection: A survey, 2019.
- [41] Yassine Himeur, Khalida Ghanem, Abdullah Alsalemi, Faycal Bensaali, and Abbes Amira. Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. *Applied Energy*, 287:116601, 2021.
- [42] Anne-Wil Harzing. *The Publish or Perish tutorial: 80 easy tips to get the best out of the Publish or Perish software*. Tarma Software Research, 2016.
- [43] Raj Mani Shukla and Shamik Sengupta. Scalable and robust outlier detector using hierarchical clustering and long short-term memory (lstm) neural network for the internet of things. *Internet of Things*, 9:100167, 2020.
- [44] Masoud Sobhani, Tao Hong, and Claude Martin. Temperature anomaly detection for electric load forecasting. *International Journal of Forecasting*, 36(2):324–333, 2020.
- [45] Mao V. Ngo, Tie Luo, Hakima Chaouchi, and Tony Q.S. Quek. Contextual-bandit anomaly detection for iot data in distributed hierarchical edge computing. In 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), pages 1227–1230, 2020.
- [46] Yu-Lin Li and Jehn-Ruey Jiang. Anomaly detection for non-stationary and non-periodic univariate time series. In 2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), pages 177–179, 2020.
- [47] Haotian Chang, Jing Feng, and Chaofan Duan. Hadiot: A hierarchical anomaly detection framework for iot. *IEEE Access*, 8:154530–154539, 2020.
- [48] Chunyong Yin, Sun Zhang, Jin Wang, and Neal N. Xiong. Anomaly detection based on convolutional recurrent autoencoder for iot time series. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pages 1–11, 2020.
- [49] Chunyong Yin, Sun Zhang, Jin Wang, and Neal N. Xiong. Anomaly detection based on convolutional recurrent autoencoder for iot time series. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pages 1–11, 2020.
- [50] Priyanga Dilini Talagala, Rob J. Hyndman, and Kate Smith-Miles. Anomaly detection in high-dimensional data. *Journal of Computational and Graphical Statistics*, 30(2):360–374, 2021.
- [51] Aysan Mahmoudzadeh, Iman Azimi, Amir M. Rahmani, and Pasi Liljeberg. Lightweight photoplethysmography quality assessment for real-time iot-based health monitoring using unsupervised anomaly detection. *Procedia Computer Science*, 184:140–147, 2021. The 12th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 4th International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops.
- [52] Rongbin Xu, Yongliang Cheng, Zhiqiang Liu, Ying Xie, and Yun Yang. Improved long short-term memory based anomaly detection with concept drift adaptive method for supporting iot services. *Future Generation Computer Systems*, 112:228–242, 2020.
- [53] Kerem Aytaç and Ömer Korçak. Iot based intelligence for proactive waste management in quick service restaurants. *Journal of Cleaner Production*, 284:125401, 2021.
- [54] Gautami Tripathi, Mohd Abdul Ahad, and Sara Paiva. Sms: A secure healthcare model for smart cities. *Electronics*, 9(7), 2020.
- [55] Takumi Asakura, Wataru Yashima, Kouki Suzuki, and Makoto Shimotou. Anomaly detection in a logistic operating system using the mahalanobis–taguchi method. *Applied Sciences*, 10(12), 2020.

- [56] Tingting Chen, Xueping Liu, Bizhong Xia, Wei Wang, and Yongzhi Lai. Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder. *IEEE Access*, 8:47072–47081, 2020.
- [57] Shaohua Huang, Yu Guo, Nengjun Yang, Shanshan Zha, Daoyuan Liu, and Weiguang Fang. A weighted fuzzy c-means clustering method with density peak for anomaly detection in iot-enabled manufacturing process. *Journal of Intelligent Manufacturing*, pages 1–17, 2020.
- [58] X.J. Zeng, M. Yang, and Y.F. Bo. Gearbox oil temperature anomaly detection for wind turbine based on sparse bayesian probability estimation. *International Journal of Electrical Power & Energy Systems*, 123:106233, 2020.
- [59] Rozhin Yasaei, Felix Hernandez, and Mohammad Abdullah Al Faruque. Iot-cad: Context-aware adaptive anomaly detection in iot systems through sensor association. In 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), pages 1–9, 2020.
- [60] Ying Cui, Jun Bao, Jinkai Wang, Qiang Zhang, and Xingke Jiang. Spatio-temporal correlation based anomaly detection and identification method for iot sensors. In 2019 International Conference on Control, Automation and Information Sciences (ICCAIS), pages 1–6, 2019.
- [61] Jun Yang, Aidong Xu, Yonggang Zeng, Li Cheng Li, Yixin Jiang, Yunan Zhang, and Hong Wen. Electricity prediction under edge devices based on sparse anomaly perception. *Journal of Physics: Conference Series*, 1659:012015, oct 2020.
- [62] Ahmed Zekry, Ahmed Sayed, Mohamed Moussa, and Mohamed Elhabiby. Anomaly detection using iot sensor-assisted convlstm models for connected vehicles. In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), pages 1–6, 2021.
- [63] Jin Wang, Yangning Tang, Shiming He, Changqing Zhao, Pradip Kumar Sharma, Osama Alfarraj, and Amr Tolba. Logevent2vec: Logevent-to-vector based anomaly detection for large-scale logs in internet of things. Sensors, 20(9), 2020.
- [64] Thien-Binh Dang, Duc-Tai Le, Tien-Dung Nguyen, Moonseong Kim, and Hyunseung Choo. Monotone split and conquer for anomaly detection in iot sensory data. *IEEE Internet of Things Journal*, pages 1–1, 2021.
- [65] Rui Hou, MingMing Pan, YunHao Zhao, and Yang Yang. Image anomaly detection for iot equipment based on deep learning. *Journal of Visual Communication and Image Representation*, 64:102599, 2019.
- [66] Aymen Yahyaoui, Takoua Abdellatif, Sami Yangui, and Rabah Attia. Read-iot: Reliable event and anomaly detection framework for the internet of things. *IEEE Access*, 9:24168–24186, 2021.
- [67] Waseem Ullah, Amin Ullah, Ijaz Ul Haq, Khan Muhammad, Muhammad Sajjad, and Sung Wook Baik. Cnn features with bi-directional lstm for real-time anomaly detection in surveillance networks. *Multimedia Tools and Applications*, 80(11):16979–16995, 2021.
- [68] Zilong Zhao, Sophie Cerf, Robert Birke, Bogdan Robu, Sara Bouchenak, Sonia Ben Mokhtar, and Lydia Y Chen. Robust anomaly detection on unreliable data. In 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pages 630–637, 2019.
- [69] Xinlin Wang and Sung-Hoon Ahn. Real-time prediction and anomaly detection of electrical load in a residential community. *Applied Energy*, 259:114145, 2020.
- [70] Anusha Koduru, M. Brihadh, R.K. Jayanth, N. Siri Chandana, K. Tej kiran, G. Vijay Kiran, and M. Prudhvi T Reddy. Geographic anomaly detection using iot principles. *Materials Today: Proceedings*, 2020.
- [71] Hakan Kayan, Yasar Majib, Wael Alsafery, Mahmoud Barhamgi, and Charith Perera. Anoml-iot: An end to end re-configurable multi-protocol anomaly detection pipeline for internet of things. *Internet of Things*, page 100437, 2021.
- [72] Enkhtur Tsogbaatar, Monowar H. Bhuyan, Yuzo Taenaka, Doudou Fall, Khishigjargal Gonchigsumlaa, Erik Elmroth, and Youki Kadobayashi. Del-iot: A deep ensemble learning approach to uncover anomalies in iot. *Internet of Things*, 14:100391, 2021.
- [73] Yisroel Mirsky, Tomer Golomb, and Yuval Elovici. Lightweight collaborative anomaly detection for the iot using blockchain. *Journal of Parallel and Distributed Computing*, 145:75–97, 2020.
- [74] Yufei An, F. Richard Yu, Jianqiang Li, Jianyong Chen, and Victor C. M. Leung. Edge intelligence (ei)-enabled http anomaly detection framework for the internet of things (iot). *IEEE Internet of Things Journal*, 8(5):3554–3566, 2021.

- [75] Yi Liu, Sahil Garg, Jiangtian Nie, Yang Zhang, Zehui Xiong, Jiawen Kang, and M. Shamim Hossain. Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 8(8):6348–6358, 2021.
- [76] Francesco Cauteruccio, Luca Cinelli, Enrico Corradini, Giorgio Terracina, Domenico Ursino, Luca Virgili, Claudio Savaglio, Antonio Liotta, and Giancarlo Fortino. A framework for anomaly detection and classification in multiple iot scenarios. *Future Generation Computer Systems*, 114:322–335, 2021.
- [77] Kashif Naseer Qureshi, Gwanggil Jeon, and Francesco Piccialli. Anomaly detection and trust authority in artificial intelligence and cloud computing. *Computer Networks*, 184:107647, 2021.
- [78] Meng Li, Keli Zhang, Jiamou Liu, Hanxiao Gong, and Zijian Zhang. Blockchain-based anomaly detection of electricity consumption in smart grids. *Pattern Recognition Letters*, 138:476–482, 2020.
- [79] Zhongguo Yang, Weilong Ding, Zhongmei Zhang, Han Li, Mingzhu Zhang, and Chen Liu. A service selection framework for anomaly detection in iot stream data. In 2020 International Conference on Service Science (ICSS), pages 155–161, 2020.
- [80] Amin Shahraki, Amir Taherkordi, and Øystein Haugen. Tonta: Trend-based online network traffic analysis in ad-hoc iot networks. *Computer Networks*, 194:108125, 2021.
- [81] E. Laxmi Lydia, A. Arokiaraj Jovith, A. Francis Saviour Devaraj, Changho Seo, and Gyanendra Prasad Joshi. Green energy efficient routing with deep learning based anomaly detection for internet of things (iot) communications. *Mathematics*, 9(5), 2021.
- [82] Meng Shen, Xiangyun Tang, Liehuang Zhu, Xiaojiang Du, and Mohsen Guizani. Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. *IEEE Internet of Things Journal*, 6(5):7702–7712, 2019.
- [83] Aditya Kumar Pathak, Saguna Saguna, Karan Mitra, and Christer Åhlund. Anomaly detection using machine learning to discover sensor tampering in iot systems. In *ICC 2021 IEEE International Conference on Communications*, pages 1–6, 2021.
- [84] Viraaji Mothukuri, Prachi Khare, Reza M. Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, and Gautam Srivastava. Federated learning-based anomaly detection for iot security attacks. *IEEE Internet of Things Journal*, pages 1–1, 2021.
- [85] Aikaterini Protogerou, Stavros Papadopoulos, Anastasios Drosou, Dimitrios Tzovaras, and Ioannis Refanidis. A graph neural network method for distributed anomaly detection in iot. *Evolving Systems*, 12(1):19–36, 2021.
- [86] S Venkatraman, P Muthusamy, Bhanuchander Balusa, T Jayasankar, G Kavithaa, KR Sekar, and C Bharatiraja. Time dependent anomaly detection system for smart environment using probabilistic timed automaton. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–9, 2021.
- [87] Abdel Mlak Said, Aymen Yahyaoui, and Takoua Abdellatif. Efficient anomaly detection for smart hospital iot systems. *Sensors*, 21(4), 2021.
- [88] K.S. Niraja and Sabbineni Srinivasa Rao. A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance iot security. *Materials Today: Proceedings*, 2021.
- [89] Maria A. Fouad and Amr Talaat Abdel-Hamid. On detecting iot power signature anomalies using hidden markov model (hmm). In 2019 31st International Conference on Microelectronics (ICM), pages 108–112, 2019.
- [90] Amaal Al Shorman, Hossam Faris, and Ibrahim Aljarah. Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for iot botnet detection. *Journal of Ambient Intelligence and Humanized Computing*, 11(7):2809–2825, 2020.
- [91] Wenguang Song, Mykola Beshley, Krzysztof Przystupa, Halyna Beshley, Orest Kochan, Andrii Pryslupskyi, Daniel Pieniak, and Jun Su. A software deep packet inspection system for network traffic analysis and anomaly detection. *Sensors*, 20(6), 2020.
- [92] Ly Vu, Van Loi Cao, Quang Uy Nguyen, Diep N. Nguyen, Dinh Thai Hoang, and Eryk Dutkiewicz. Learning latent representation for iot anomaly detection. *IEEE Transactions on Cybernetics*, pages 1–14, 2020.
- [93] Nour Moustafa, Marwa Keshk, Kim-Kwang Raymond Choo, Timothy Lynar, Seyit Camtepe, and Monica Whitty. Dad: A distributed anomaly detection system using ensemble one-class statistical learning in edge networks. *Future Generation Computer Systems*, 118:240–251, 2021.
- [94] Qasem Abu Al-Haija and Saleh Zein-Sabatto. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics*, 9(12), 2020.
- [95] Paweł Dymora and Mirosław Mazurek. An innovative approach to anomaly detection in communication networks using multifractal analysis. *Applied Sciences*, 10(9), 2020.

- [96] Amir Basati and Mohammad Mehdi Faghih. Apae: an iot intrusion detection system using asymmetric parallel auto-encoder. *Neural Computing and Applications*, pages 1–21, 2021.
- [97] Chao Wang. Iot anomaly detection method in intelligent manufacturing industry based on trusted evaluation. *The International Journal of Advanced Manufacturing Technology*, pages 1–13, 2019.
- [98] Debasmita Mishra, Bighnaraj Naik, Pandit Byomakesha Dash, and Janmenjoy Nayak. Sem: Stacking ensemble meta-learning for iot security framework. Arabian Journal for Science and Engineering, 46(4):3531–3548, 2021.
- [99] MPS Bhatia and Saurabh Raj Sangwan. Soft computing for anomaly detection and prediction to mitigate iot-based real-time abuse. *Personal and Ubiquitous Computing*, pages 1–11, 2021.
- [100] Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang. Real-time nonparametric anomaly detection in high-dimensional settings. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(7):2463–2479, 2021.
- [101] Jiaxin Du, Guangjie Han, Chuan Lin, and Miguel Martinez-Garcia. Itrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*, pages 1–1, 2020.
- [102] Chunde Liu, Xianli Su, and Chuanwen Li. Edge computing for data anomaly detection of multi-sensors in underground mining. *Electronics*, 10(3), 2021.
- [103] Yongliang Cheng, Yan Xu, Hong Zhong, and Yi Liu. Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in iot communication. *IEEE Internet of Things Journal*, 8(1):144–155, 2021.
- [104] Nickolaos Koroniotis;, Nour Moustafa;, Elena Sitnikova;, and Benjamin Turnbull. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100:779–796, 2019.
- [105] Meng Shen, Xiangyun Tang, Liehuang Zhu, Xiaojiang Du, and Mohsen Guizani. Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. *IEEE Internet of Things Journal*, 6(5):7702–7712, 2019.
- [106] Sahil Garg, Kuljeet Kaur, Neeraj Kumar, and Joel J. P. C. Rodrigues. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in sdn: A social multimedia perspective. *IEEE Transactions on Multimedia*, 21(3):566–578, 2019.
- [107] Mingtao Wu, Zhengyi Song, and Young B Moon. Detecting cyber-physical attacks in cybermanufacturing systems with machine learning methods. *Journal of intelligent manufacturing*, 30(3):1111–1123, 2019.
- [108] Shadi A Aljawarneh and Radhakrishna Vangipuram. Garuda: Gaussian dissimilarity measure for feature representation and anomaly detection in internet of things. *The Journal of Supercomputing*, 76(6):4376–4413, 2020.
- [109] Xiaokang Zhou, Yiyong Hu, Wei Liang, Jianhua Ma, and Qun Jin. Variational lstm enhanced anomaly detection for industrial big data. *IEEE Transactions on Industrial Informatics*, 17(5):3469–3477, 2021.
- [110] Kobra Mabodi, Mehdi Yusefi, Shahram Zandiyan, Leili Irankhah, and Reza Fotohi. Multi-level trust-based intelligence schema for securing of internet of things (iot) against security threats using cryptographic authentication. *The Journal of Supercomputing*, pages 1–26, 2020.
- [111] Zhihan Lv, Yang Han, Amit Kumar Singh, Gunasekaran Manogaran, and Haibin Lv. Trustworthiness in industrial iot systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics*, 17(2):1496–1504, 2021.
- [112] Ivan Cvitić, Dragan Peraković, Marko Periša, and Mate Botica. Novel approach for detection of iot generated ddos traffic. *Wireless Networks*, 27(3):1573–1586, 2021.
- [113] Wei Liang, Lijun Xiao, Ke Zhang, Mingdong Tang, Dacheng He, and Kuan-Ching Li. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet of Things Journal*, pages 1–1, 2021.
- [114] Will Serrano. The blockchain random neural network for cybersecure iot and 5g infrastructure in smart cities. *Journal of Network and Computer Applications*, 175:102909, 2021.
- [115] Francesco Cauteruccio, Luca Cinelli, Enrico Corradini, Giorgio Terracina, Domenico Ursino, Luca Virgili, Claudio Savaglio, Antonio Liotta, and Giancarlo Fortino. A framework for anomaly detection and classification in multiple iot scenarios. *Future Generation Computer Systems*, 114:322–335, 2021.

- [116] Menglin Dai, Wil O.C. Ward, Gregory Meyers, Danielle Densley Tingley, and Martin Mayfield. Residential building facade segmentation in the urban environment. *Building and Environment*, 199:107921, 2021.
- [117] Jie Lu, Anjin Liu, Fan Dong, Feng Gu, João Gama, and Guangquan Zhang. Learning under concept drift: A review. *IEEE Transactions on Knowledge and Data Engineering*, 31(12):2346–2363, 2019.
- [118] Haodong Lu, Miao Du, Kai Qian, Xiaoming He, and Kun Wang. Gan-based data augmentation strategy for sensor anomaly detection in industrial robots. *IEEE Sensors Journal*, pages 1–1, 2021.