Future Generation Computer Systems 134 (2022) 170–186

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Review article

A systematic literature review of IoT time series anomaly detection solutions

Arnaldo Sgueglia *, Andrea Di Sorbo, Corrado Aaron Visaggio, Gerardo Canfora

Department of Engineering, University of Sannio, Benevento, 82100, Italy

ARTICLE INFO

Article history:
Received 18 November 2021
Received in revised form 24 March 2022
Accepted 8 April 2022
Available online 16 April 2022

Keywords:
IoT
Internet of Things
Anomaly detection
Time series

ABSTRACT

The rapid spread of the Internet of Things (IoT) devices has prompted many people and companies to adopt the IoT paradigm, as this paradigm allows the automation of several processes related to data collection and monitoring. In this context, the sensors (or other devices) generate huge amounts of data while monitoring physical spaces and objects. Therefore, the problem of managing and analyzing these huge amounts of data has stimulated researchers and practitioners to adopt anomaly detection techniques, which are automated solutions to enable the recognition of abnormal behaviors occurring in complex systems. In particular, in IoT environments, anomaly detection very often involves the analysis of time series data and this analysis should be accomplished under specific time or resource constraints. In this systematic literature review, we focus on the IoT time series anomaly detection problem by analyzing 62 articles written from 2014 to 2021. Specifically, we explore the methods and techniques adopted by researchers to deal with the issues related to dimensionality reduction, anomaly localization, and real-time monitoring, also discussing the datasets used, and the real-case scenarios tested. For each of these topics, we highlight potential limitations and open issues that need to be addressed in future work.

Contents

1. Introduction

In the last decade, Internet of Things (IoT) has attracted intensive attention due to a wide range of applications in industrial,

* Corresponding author.
E-mail addresses: sgueglia@unisannio.it (A. Sgueglia), disorbo@unisannio.it (A. Di Sorbo), visaggio@unisannio.it (C.A. Visaggio), canfora@unisannio.it (G. Canfora).

https://doi.org/10.1016/j.future.2022.04.005
0167-739X/

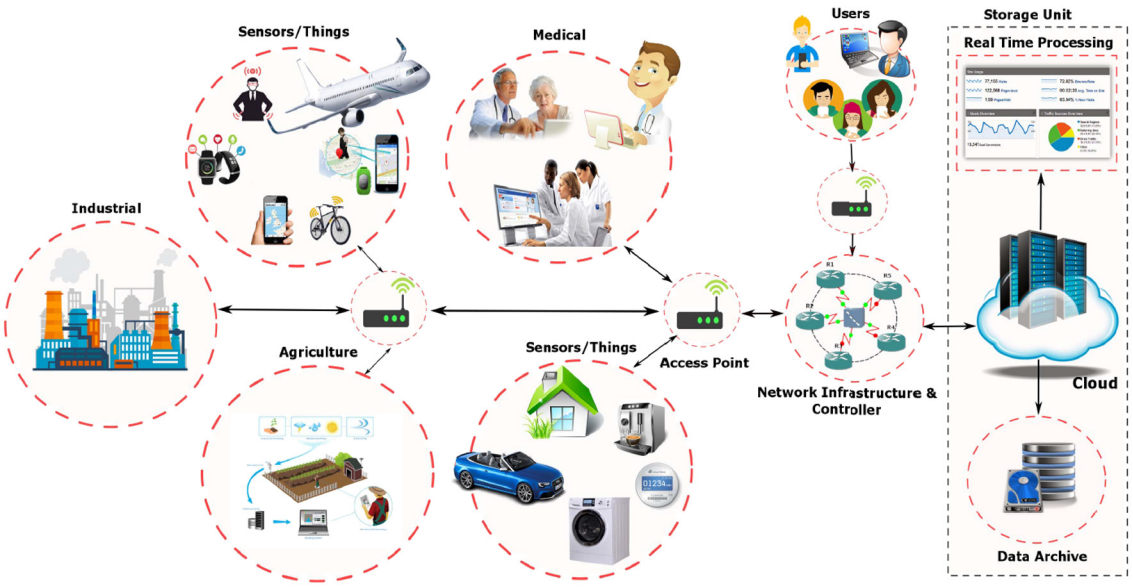


Fig. 1. Internet of Things (IoT) architecture.

biomedical observation, agriculture, smart cities, environmental monitoring and other fields (see Fig. 1) [1].

Indeed, the rapid spread of the Internet of Things (IoT) devices has prompted many people and companies to adopt the IoT paradigm, as this paradigm allows the automation of several processes related to data collection and monitoring [2].

Despite this, several issues still affect these devices. In particular, the main IoT issues can be divided into two main categories: standards (i.e. energy consumption, devices heterogeneity, and standardization) and more related to the anomaly detection techniques (i.e. privacy and security, availability, and fault tolerance), described as follow:

- **Energy consumption:** most of the IoT devices are battery-powered, and this leads to the reduction of the unuseful wasting energy by unnecessary data transmissions, protocol overheads, or running the radio all the time (listening and transmitting). IoT technology will soon enable the realization of self-sustainable wireless communication. IoT devices vendors are working on these issues by including several additional energy sources such as wind-solar, thermal energy, kinetic energy, hydroelectric harvesting. Therefore, it is necessary to optimize the energy consumption of a system;
- **Devices heterogeneity:** IoT combines a multitude of devices and infrastructures which operate with their architectures, protocol stacks, and data formats. This integration has created complex interoperability and integration challenges to realize large-scale heterogeneous IoT ecosystems. The communications between these heterogeneous devices need to be adaptive to allow dynamic interconnectivity and support decentralized nature [1];
- **Standardization:** standardization of IoT architecture and communication technologies are viewed as a backbone for IoT development in the future. That brings researchers to think about open standards as one of the key factors for the successful deployment of IoT. The usage of open standards leads to several advantages, such as (i) being a great facilitator for innovation due to their public availability, and (ii) less chance of being limited to a specific vendor or technology. The scopes of standardization activities are various to provide open standards and architectures, seamless connectivity, and interoperability;
- **Privacy and security:** security and privacy are intrinsic parts of IoT networks. It is fundamental to ensure privacy protection and security in various activities, such as transportation, personal activities, business processes, and information protection. IoT systems are also desired to be self-healing (detect, diagnose, and countermeasure the attack). There is a wealth of literature on securing IoT systems, but networks are still suffering from threats and are being hacked frequently;
- **Availability:** services' availability is one of the fundamental issues to be addressed to manage IoT systems dynamics. An appropriate monitoring system, protocols, and self-healing mechanisms are required to enable systems robustness. In the mobility scenario, devices can be freely moved and frequent topology changes can occur. The goal is to create a robust system despite these dynamic changes. Also, some deployments of IoT systems imply that sensors need to know their locations and be aware of their environment (neighbor devices' location) [3];
- **Fault tolerance:** it is one of the most important issues for WSN and IoT applications. Some sensor nodes may be blocked or fail due to environmental interference, physical damage, or lack of power. Most routing protocols can recover from the failure of a sensor node. The problem becomes worse when two or more sensor nodes fail in the same area. The network might cripple because other nodes might not find a route to the ultimate receiver. Therefore, a routing protocol must follow new links dynamically to deliver the data collected by other devices to the intended destination.

Although these limitations are still present, researchers need to analyze increasing amounts of data. Specifically, the growing adoption of IoT devices entails an ever greater increase in the volumes of data that need to be processed and analyzed [4]. In particular, gaining useful information from these large volumes of data without the help of automated approaches becomes infeasible. In addition, even when automated approaches are available, the data analysis might require too much time due to the large volumes of data that are continuously generated by IoT devices, with the risk of hampering monitoring tasks [5]. To address these problems, anomaly detection technologies have been introduced

with the aim of improving the data collection and analysis processes. Anomaly detection establishes whether the data collected or produced by the devices reflect the expected behavior by signaling the occurrence of events that deserve attention.

Real-life systems are continuously affected by anomalies, and timely (and precisely) identifying such anomalies can make devices more reliable and secure, avoiding the waste of valuable resources. In most cases, these systems are subject to some constraints, depending on the specific applications for which they are created. For example, in the case of IoT, it is crucial to adapt the models to collect and analyze univariate and multivariate time series and detect the different types of anomalies that may occur in time and space. A few specific techniques have been already developed to address some of the issues related to anomaly detection in time series.

These constraints highlight the necessity of better analyzing these two aspects. Firstly, our paper tries to understand which are the main methods and techniques used to deal with time-series data. The time series analysis offers several advantages such as better detection and identification of anomalies in the collected data. These advantages came from the relation between time-series data. In this context, researchers can identify every kind of anomaly in both anomalous and normal data too. Another important reason is that the research community can retrieve much complex information from environmental events that influence the whole or part of the sensor network. The reason is that, nowadays, in the field of monitoring physical and non-physical environments, the vast majority of events that influence modern device networks mostly exhibit dynamic behavior and are no longer static as they once were. The use of time series makes dealing with environmental phenomena much easier than in previous years. Secondly, the focus is on the most recent challenges and open issues in the fields of IoT anomaly detection. The aim is to provide a big picture of the challenges and open issues identified so far. It is important to collect this information since this helps the community to understand the baseline; furthermore further aspects not yet mentioned are highlighted. This could be the starting point for further research both in the field of anomaly detection and IoT-specific issues and challenges.

Although there is not a universally accepted definition of anomaly, within the context of IoT the following one can be given: *an anomaly is the set of measurable consequences of an unexpected change in the state of a system which is outside of its local or global norm* [6]. In particular, we can identify three main different types of anomalies [7]:

- **Point anomaly**: it is a point in a data distribution that is far different from the rest of the data distribution. It is also known as an "outlier". As an example, if we are monitoring the temperature in a room, a point anomaly is a point in which a high rise or a low fall of data is produced by the device;
- **Contextual anomaly**: it represents data that seems to be normal in a certain scenario, but anomalous in another one. This type of anomaly is common in time-series data streams. For example, contextual anomalies occur when monitoring the street traffic; from 6 AM to 9 AM the presence of traffic is quite normal, while from 11 PM to 4 AM it is unusual;
- **Collective anomaly**: it can be identified only after the analysis of the entire sequence of data and the extraction of the collective behavior of the data stream. Any minimum deviation from the normal behavior may lead to a collective anomaly. As an example, the heart rate monitoring can be considered; first the entire sequence to learn the normal pattern is analyzed, and only then anomalies can be detected (for example a high increase in the heart rate).

Nowadays, data from IoT devices such as sensors, machines, and wearables are often collected in the form of time series since these data are generated and transmitted with high velocity [8]. On the one hand, the time series data collected by sensing devices are the primary source for numerous data visualization and data mining (e.g., classification, clustering, prediction) purposes [9]. On the other hand, time series have distinct temporal and sequential characteristics, and special methods are necessary to perform IoT time series anomaly detection [10]. Specifically, anomaly detection in time series is becoming an increasingly important research area, as organizations more and more need to monitor time-series data to detect anomalies, thus reducing troubleshooting costs [11]. Classic anomaly detection problems usually consist of finding single data points differing from the rest of the data. Instead, time series anomaly detection techniques typically aim to find segments in the time series corresponding to unusual behaviors. In particular, time series anomaly detection allows to find anomalies whose data points are within the normal range, but they represent unusual patterns [12].

In this paper, we conduct a systematic literature review to better understand (i) the techniques addressing IoT time series anomalies developed or envisioned so far, (ii) the actual performance of such techniques in both synthetic and real scenarios, and, more importantly, (iii) the challenges and open issues that need to be addressed by future research. In particular, we pose the following general research question (RQ):

Which are the state-of-the-art techniques, their performance, and the main open issues that need to be addressed in the field of IoT time series anomaly detection?

Our work stems from a previous Systematic Literature Review of anomaly detection on IoT devices reported in [7] and aims at understanding whether (and how well) any of the issues, challenges, and gaps highlighted by the authors have been addressed. However, while previous work investigated analysis models and techniques envisioned for specific types of devices used in particular contexts (such as smart inhabitant environments, transport systems, healthcare systems, smart objects, and industrial systems), our work specifically focuses on anomaly detection in time series by addressing topics not discussed in prior work, such as dimensionality reduction, anomaly localization, and real-time systems. In particular, our work provides two main contributions: on the one hand, it gives a big picture of the current techniques, methods, and tools addressing the problem of anomaly detection using time series in the context of IoT devices; on the other hand, we identify the most critical open challenges that need to be addressed by future research.

Our results highlight several novel limitations of the current research in the area. Firstly, the few available datasets very often contain synthetic data (and not real-world ones) likely leading to incomplete assessments of the actual performance of the systems. Secondly, while robust approaches and techniques for real-time anomaly detection are still lacking, we also observed a shortage of methods for performing anomaly localization; such methods would help to identify the likely causes of the anomalies. Thirdly, we report the lack of contextual anomaly detection systems using time-series. Last but not least, the conception of advanced techniques (beyond traditional ones) for reducing the dimensionality of the data collected by the devices would certainly lead to improvements, not only in the performance of individual frameworks, but also in the available techniques, technologies, and paradigms specifically created to manage large amounts of data. Notably, as also demonstrated by the fact that we were not able to find any studies addressing some specific topics, we believe that our work has the potential of stimulating further research on several aspects related to anomaly detection in IoT environments.

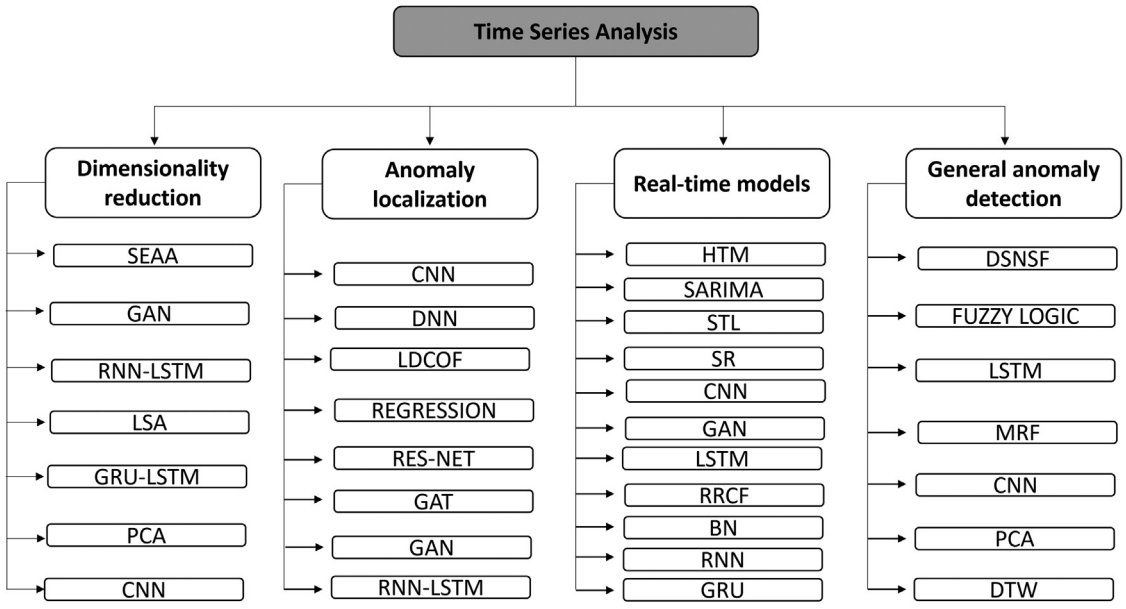


Fig. 2. Taxonomy for time series anomaly detection methods.

Fig. 2 reports all the methods used for time series analysis identified during our review. As a result of our work, four main categories are identified (i.e., dimensionality reduction, anomaly localization, real-time models, and general anomaly detection). For each category, we report the main methods to handle time-series data. This taxonomy assumes particular relevance due to its dual purpose: it highlights the main anomaly detection techniques based on time series data and provides an overview for researchers dealing with these topics.

The rest of the paper is organized as follows. In Section 2, a practical case study highlights how the anomaly detection methods work in the IoT environment and the practical advantages of using time series models in the IoT field. The existing studies about IoT anomaly detection, such as surveys or other previous systematic literature reviews, are discussed and compared in Section 3. Section 4 deals with the research methodology we followed, while Section 5 reports the findings of our review. Section 6 discusses the open issues identified, while conclusions are drawn in Section 7.

2. Motivating example

This section presents a practical case study to show how anomaly detection methods work in IoT. The considered case study refers to the identification of activities carried out by people. Human activities recognition (HAR) has become a popular topic in the last decades due to its importance for many areas, including healthcare, interactive gaming, sports, and general-purpose monitoring systems [13]. Nowadays, the aging population is becoming one of the world's primary concerns. It was estimated that the population aged over 65 would increase from 461 million to 2 billion by 2050. This substantial increase will have significant social and healthcare consequences. The goal of HAR is to recognize human activities in controlled and uncontrolled settings.

Most of the data used by the algorithms in this context come from both environmental and embedded sensors. In the former case, the nature of these sensors ranges from simple temperature sensors to the most complex environmental sensors such as cameras placed in strategic locations for detection purposes. In the case of embedded sensors, instead, the sensors are integrated in clothing or medical equipment. The introduction of IoT devices has given rise to a world full of internet-connected devices capable of continuously generating data. This increasingly widespread paradigm has now become a transversal technology with a large number of application scenarios. In particular, the increasing amount of generated data enables the possibility to collect and analyze it to obtain meaningful information.

One application includes the monitoring of people's activities. In this specific context, anomaly detection systems play a crucial role. The base idea behind this application is that IoT devices are used to collect physical parameters of the subjects wearing them and process such parameters through a set of algorithms capable of detecting anomalous conditions. The introduction of time-series models expands the anomaly detection possibilities and leads to improvements in the identification process. Among the advantages provided by time series in anomaly detection systems, there is the possibility of exploiting the relationships between data, which is not always possible with the standard methods and techniques used so far. This aspect highlights the opportunities of analyzing new types of anomalies, such as contextual anomalies. In this context, the first step in dealing with this new type of anomaly is to encode the data context in the data representation itself.

Standard anomaly detection systems mainly detect anomalies concerning outliers in the data. Beyond detecting outliers, time-series-based models allow determining whether an event can be considered an anomaly (or not) given a specific context. For example, let us consider the two actions of *sleep* and *work*. In a standard scenario, a data analyst will only be able to determine the presence or absence of outliers, instead, in the case of time series and contextual anomalies, a data analyst will be able to determine the presence or absence of outliers and, in addition, will also be able to determine whether, in a given time slot, an action will be considered anomalous or not. For instance, in a time slot between 11 PM and 7 AM, the sleeping action will be regarded as not abnormal. Instead, the same action in the time slot between 11 AM and 1 PM of a working day might be considered abnormal. Similarly, a sudden change from a vertical to a horizontal position of a person walking in a public location during daytime might indicate that the person felt ill.

Table 1
Main differences between our study and previous ones.

Dimensions	Our study	Fakhrazari and Vakilzadian [14]	Fahim and Sillitti [7]	Ali et al. [15]	Gaddam et al. [16]	Sharma et al. [17]	Cook et al. [6]	Dwivedi et al. [18]
Study type	Slr	Survey	Slr	Survey	Survey	Survey	Survey	Survey
Data type	Time series	Time series	Time series	Time series	Time series	Time series	N/A	N/A
Analysis techniques	✓	✓	✓	✓	✓	✓	✓	✓
Available datasets	✓							
Challenges/Open issues for analysis techniques	✓	✓	✓	✓	✓	✓	✓	✓
Challenges/Open issues for anomaly detection applied to IoT devices operations	✓							
Challenges/Open issues for applications	✓	✓	✓	✓	✓	✓	✓	
Dimensionality reduction	✓							
Anomaly localization	✓							
Real-time models	✓							

3. Related work

There is a growing interest in problems regarding anomaly detection on IoT systems. In [14], the authors highlighted current possible representations of data, measures of similarity between them, and created a taxonomy of the most common mining tasks. Their analysis showed that there has been a gradual migration of interest from single data management systems towards whole data streams. The survey presented by Ali et al. [15] identified the time-series (i.e., the data produced by the sensors in a certain time frame) usages and evaluated the various types of time-series data structures, the similarity measures introduced so far, and, finally, focused on the methods for analyzing the time series, reporting several studies on classification and clustering tasks.

In [16], the authors first focused on the sources that generate outliers and anomalies, and then moved to the evaluation of failure classification techniques and the identification of outliers. Sharma et al. [17] highlighted the necessity of frameworks that can handle real-time outlier detection and analysis on data streams. Subsequently, Cook et al. [6] proposed a set of methods useful for analyzing univariate and multivariate time series. Moreover, they identified numerous challenges affecting real-time analysis systems, windowed or incremental approaches to partition data, supervised or unsupervised models, multivariate time-series, and generalized approaches for the design of tools and frameworks.

In a similar effort, Dwivedi et al. [18] analyzed several studies on supervised and unsupervised learning approaches, and observed that the best algorithms are those using PCA to reduce dimensionality and density-based methods for analysis. Finally, in [7] the researchers identified the best methods and metrics to analyze data and to evaluate the performance of systems for smart inhabitant environments, transportation systems, health care systems, smart objects and industrial systems. They concluded by listing some of the unsolved challenges and carrying out a so-called gap analysis. Among the most important challenges, they mentioned the imbalance of the data produced (e.g., normal and anomalous data rate, the quality of data, etc.), the need for new representations to manage data complexity, and to deal with collective and contextual anomalies. In their gap analysis, they also observed a limited and long processes for accessing the datasets, systems trained only on normal data, many parameters to manage, no studies about data fusion.

Unlike prior studies, we focus our review on specific aspects of time-series anomaly detection in IoT contexts, such as dimensionality reduction, anomaly localization techniques, and real-time models and tools. In particular, beyond analyzing the main studies presented so far, we also identify the main challenges and open issues that need to be addressed by future research.

Table 2
Survey description.

Author(s)	Description	Findings
Fakhrazari and Vakilzadian [14]	Identified actual data representation, similarity measures and most common mining task	Lack of frameworks for mining and analysis of streams of data
Ali et al. [15]	Focus on time series data; similarity measures, methods of time series analysis and classification	Report some of the methods to extract and analyze time series
Gaddam et al. [16]	Focus on IoT sources of anomalies	Highlight pros and cons of the considered analysis and detection methods
Sharma et al. [17]	Describe some challenges of IoT devices	Highlight the need of real time frameworks to manage real world systems
Cook et al. [6]	Focus on techniques to analyze Univariate and Multivariate time series and some challenges	Highlight the need of real-time solutions, multivariate data and generalized approaches
Dwivedi et al. [18]	Report some studies on Unsupervised and Supervised approaches	The best solutions use PCA and density based methods
Fahim and Sillitti [7]	Analyze anomaly detection problem about IoT systems	Report some issues and gap found so far

Table 1 points out the differences between our study and recent work on the same topic for the considered dimensions. We grouped the dimensions into information related to study characteristics and topics surveyed in our study. The characteristics refer to study type (i.e. **S**ystematic **L**iterature **R**eview or Survey) and the data type analyzed in the paper. The topics concern: Analysis techniques, Available dataset, Challenges/Open issues for analysis techniques, Challenges/Open issues for anomaly detection applied to IoT devices operations, and Challenges/Open issues for applications. Looking at Table 1, it is clear that the proposed work focuses both on already studied and new topics. On the one hand, it uses the already studied topics as a baseline to provide a strong background in supporting further analysis. On the other hand, instead, the proposed work focuses on topics not discussed in prior work, such as (i) a description of the most used datasets, (ii) challenges and open issues for anomaly detection applied to IoT devices operations, and (iii) the three topics specifically explored in our proposed work (i.e., dimensionality reduction, anomaly localization, and real-time models).

In addition, in Table 2 we provide an overview of the selected surveys on the topic.

4. Research methodology

This systematic literature review on time series anomaly detection for IoT devices and sensors follows the guidelines of Kitchenham and Charters in [19].

This research study focuses on the investigation of existing and proposed methods and techniques to deal with time series models applied to the IoT anomaly detection field. The reach of this goal requires an initial basic knowledge of the IoT anomaly detection models based on time series. Subsequently, it needs to understand the main challenges and open issues which affect devices and sensors in this context. After that, it focuses on the main methods and techniques introduced so far to deal with these relevant issues. Finally, our interest aims to evaluate the main models adopted by researchers to manage devices and sensors in this field.

In this section, we explain how the papers mentioned in this review have been selected, prepared, and analyzed. Moreover, we show how those papers are distributed over time and over the different types of publications. In particular, we summarize these details in Tables 3 and 4, respectively.

Table 3
Summary of articles divided by years.

Year	# Articles	% Articles
2014	2	3,22%
2015	2	3,22%
2016	4	6,45%
2017	6	9,68%
2018	9	14,52%
2019	17	27,42%
2020	16	25,81%
2021	6	9,68%

Table 4
Summary of articles divided by publication type.

Sites	# Articles	% Articles
Conference	27	43,55%
Journal	24	38,71%
Preprint	7	11,30%
Symposium	2	3,22%
Workshop	2	3,22%

4.1. Selection of primary study

To address the primary study issue, the following search strings: "IoT time series anomaly detection" AND "IoT multivariate time series anomaly detection" are identified and restricted the search to the years from 2017 to 2021. However, we immediately realized that only a few studies relevant for this topic were found. For this reason, we had to extend the time range to the years from 2014 to 2021.

After conducting a set of preliminary searches, it was found that using only the first search string results mainly included articles referred to univariate time series. Therefore, to consider studies on both univariate and multivariate time series, it was necessary to take into account the second search string focused on multivariate time series.

The following platforms were used for the search: ACM Digital Library,[1] Google Scholar,[2] Science Direct[3] and IEEE Xplore Digital Library.[4]

To search the selected platforms, our strategy is to use both manual and automatic search. Automatic search is realized through entering search strings on the search engines of the electronic data source. Manual search is realized through manually browsing the conferences, journals or other important sources. The manual searches appeared to be quite useful since we retrieved some good-quality articles that an automatic search could not reveal [20].

For each paper found, we analyzed the title, the abstract, and the conclusion section to determine if it was suitable for being included in our review. We further examined the other sections of the suitable documents to identify the paper's main contributions and limitations.

4.2. Inclusion and exclusion criteria

The considered inclusion criteria are (i) the number of citations, (ii) the quality of the realized publications and (iii) the quality of the publication sites. For all the resultant papers, we take into account both the quality of the publication site and the quality of the realized publications. In particular, for the articles in the time range 2014 to 2019, we required a minimum number of citations (i.e. 10 or more). Instead, for the papers in the time range from 2020 to 2021 we decided not to consider the number of citations, given they were recent works, and we looked at the quality of the realized publications and to the quality of publication sites. Concerning the quality of the realized publication, we mainly looked at the following characteristics: stated goals, adherence to the topics proposed in our study, meaningful contributions, and future directions.

Achieving 10 or more citations means that these works have been taken into real consideration by the research community and can be used as references for future research.

The results are filtered on the following exclusion criteria: (i) the quality of the publication site, (ii) the quality of the proposed study, (iii) the focus of the paper, and (iv) the language used. As regards the quality of the publication site, only papers published in scientific international journals, international conferences, archive articles, workshops, and symposiums were considered, while all other kinds of sources and works like books, technical reports or master thesis were not included in this work. Moreover, we excluded papers that were not strictly related to the core of our analysis, in particular, those related to anomaly detection that does not concern time series and IoT devices. Finally, we did not consider articles written in languages different from English.

4.3. Quality assessment

Regarding the quality assessment, the studies were divided into the following four categories:

- Dimensionality reduction techniques;
- Anomaly localization models;
- Real-time anomaly detection systems;
- General anomaly detection frameworks.

4.4. Data extraction and analysis

In order to analyze the 62 articles, we broke them down into constituent parts based on a specific set of characteristics feeding back to our research question. For each paper that passed the quality assessment phase, we have examined the following further aspects: the motivations, the contribution to research, the results, and the challenges highlighted for future work. Finally, a spreadsheet was created to report the following details about each identified paper:

[1] https://dl.acm.org/.
[2] https://scholar.google.com/.
[3] https://www.sciencedirect.com/.
[4] https://ieeexplore.ieee.org/Xplore/home.jsp.

Table 5
Articles about dimensionality reduction.

Author	Method used	Description	Experimental dataset	Validation techniques	Findings
Krawczak and Szkatuła [21]	ML	Create a new symbolic representation of the original data series	UCI	Empirical	Alternative technique to PCA. It achieves an accuracy of 98% with one-nearest-neighbor algorithm and Euclidean distance
de Souza et al. [22]	ML	Use an heuristics that may help in data management and process efficiency	Forest Cover	Empirical	Propose heuristics useful in a WSN scenario that allow an increasing of accuracy of 72% and a reduction of power consumption and temperature of 18% and 15% respectively
Feremans et al. [23]	ML	Focus on Pattern-based anomalies	NAB	Empirical	Capable of manage mixed-types anomalies. Achieves an AUROC of 81% and an AP of 65% on univariate time series and an AUROC of 93% and an AP of 73% on multivariate time series
Bosman et al. [24]	DL	Focus on detecting anomalies at sensor node level	Grand St. Bernard, Intel Lab	Empirical	Describe an approach to use neighborhood information. It shows that recall benefits from neighbor information while precision does not
Moshtaghi et al. [25]	ML	New approach to cluster data	Synthetic Locally Linear Process, Shifting Gaussian Distribution, Real-life dataset	Empirical	New online clustering algorithm. It achieves a Rand Index of 90% and outperforms other compared algorithms
Li et al. [26]	DL	Apply PCA method to reduce dimensionality	SWaT	Empirical	Employ RNN-LSTM algorithm as Discriminator and Generator. It achieves a precision between 80%–90% for univariate and a precision between 90%–94% for multivariate time series
Su et al. [27]	DL	Capture normal pattern by learning representation by using stochastic variables and planar normalizing flow	SMD, SMAP, MSL	Empirical	Outperforms method LSTM-NDT, DAGMM and LSTM-VAE-based systems with a precision of 78%, recall of 96% and F1 score of 86%
Takeishi and Yairi [28]	DL	Approach for dimensionality reduction with sparse representation	Custom	Empirical	Reaches an AUC of 96%, 80% and 61% while PCA reaches only 68%, 75% AND 57% on the three experiments; but considers only a few features
Zhang et al. [29]	DL	Propose a network dual-window method to detect periodic IoT time series	UCR/UEA, NAB, Yahoo Webscope	Case study	Outperforms other state of art algorithms with precision, recall and F1-score between 90–99%
Hyndman et al. [30]	ML	Identify a subset of features from time series and through PCA method select only the first two	Yahoo Webscope, Custom	Empirical	Used with large dataset of time series; achieves an average precision of 80%

- Article metadata (e.g., title, authors, year, etc.);
- Method used;
- Description;
- Experimental dataset;
- Validation techniques;
- Article type (e.g., conference paper, journal paper, etc.).

These details have been used to more easily organize the discussion of the results, making clearer the studies' similarities and differences.

4.5. Selection results

The two identified search strings are used to search for relevant articles in the platform mentioned in Section 4.1. The search engines are configured to (i) retrieve articles published from 2014 to 2021 and (ii) search in the title, abstract, and keywords fields. Using the mentioned search strings, we got the following results:

- ACM Digital Library: 226,146 results;
- Google Scholar: 17,700 results;
- Science Direct: 245 results;
- IEEE Xplore Digital Library: 9 results.

After the application of the inclusion and exclusion criteria, we identified 62 papers. To ease the analysis of such papers, we performed the quality assessment procedure and classified the selected articles into the categories listed in Section 4.3.

5. Results

Table 3 reports a summary of the reviewed articles sorted by publication year, while Table 4 groups them by publication types. In the next few subsections, we provide a complete overview of the whole work. In particular, the "Method used" field in Tables from 5 to 8 can assume one of the two possible values: ML or DL, which refers to Machine Learning and Deep Learning techniques, respectively. Specifically, in Table 5 we list the articles about dimensionality reduction solutions, in Table 6 those about anomaly localization models, in Table 7 those about real-time systems, and in Table 8 those about general anomaly detection framework.

5.1. Dimensionality reduction

In this subsection, we discuss dimensionality reduction. An overview of the selected articles on this topic is provided in Table 5. Krawczak and Szkatuła [21] propose an approach based on the SEAA (Symbolic Essential Attributes Approximation) that is based on the concept of data series envelopes and essential attribute generation. This approach demonstrates the ability to

Table 6
Articles about anomaly localization.

Author	Method used	Description	Experimental dataset	Validation techniques	Findings
Ding et al. [31]	DL	Propose a model based on LSTM and GMM models	NAB, Custom	Empirical	Use a health factor to understand the classification level of the proposed framework. Achieve precision, recall, and F1-score values of 90%, 93%, and 91%, respectively
Kim and Cho [32]	DL	Propose a window-based method to extract features from IoT time series	Yahoo Webscope	Empirical	Outperform other state of art algorithms in term of precision (98,7%) and recall (98,5%)
Zhang et al. [33]	DL	Construct a multi-scale signature matrices to characterize multiple levels of the system statuses in different time step	Custom	Empirical	Outperform GMM and CNN based models. Achieve precision, recall, and F1-score values of 100%, 80%, and 89% on synthetic data and 80%, 85%, and 82% on real-world data
Wang et al. [34]	ML	Propose a self-learning online algorithm to identify anomalies and locate them	Dutch Power consumption data, Intel Production dataset 1,2	Case study	Automate the tuning phase by applying some methods to sliding windows and clusters
Wen and Keyes [35]	DL	Propose a Time series segmentation approach and a network architecture for multivariate time series	Dodgers Loop Sensor, Gasoil Plant Heating Loop	Empirical	Possibility to use pre-trained models with transfer learning. The approach achieves a precision of 92%
Giannoni et al. [36]	ML	Propose and evaluate several algorithm for anomaly detection	SWaT	Case study	Local Density Cluster-based Outlier factor give the best performance, achieving precision, recall, and F1-score values of 69%, 75%, and 72%, respectively
He et al. [37]	DL	Propose a neural network capable of identify variable association anomaly and locate them	Custom	Empirical	Outperform other state of art algorithms; obtain AUPR and AUROC values of 75% and 89%, respectively
Goh et al. [38]	DL	Propose an approach to detect cyber attack to the Cyber–Physical-Systems	SWaT	Case study	Unsupervised learning approach different from specification or signature based methods
Yasaei et al. [39]	DL	Propose an adaptive context-aware anomaly detection method based on sensor fingerprint generation	Custom	Empirical	The proposed method may identify anomalies with the highest precision rate, providing the possibility to update it in case of variations; it achieves precision, recall, and F1-score values of 92%, 70%, and 50%, respectively
Munir et al. [40]	DL	Propose a Unsupervised CNN-based model to detect periodic IoT time series	NAB, Yahoo Webscope	Empirical	General framework capable of detecting point and contextual anomalies. It achieves, in some cases, lower values than state-of-art algorithms but with a minimal difference between precision and recall values
He et al. [41]	DL	Propose an unsupervised method based on multiscale convolution and graph attention techniques	MSL, SMAP, SMD	Empirical, Case study	Thanks to GAT techniques it is useful in anomaly localization; It achieves precision, recall, and F1-score values from 89 to 97% but recall is lower than other algorithms
Hsieh et al. [42]	DL	Propose a real-time unsupervised model to detect anomalies at early stage of production	Custom	Empirical, Case study	Outperform other state of art algorithms with precision, recall, and F1-score of 90%, 89%, and 90%, respectively
Yin et al. [10]	DL	Propose a dual-window-based method to extract periodic IoT time series	Yahoo Webscope	Empirical	Outperform other state of art algorithms with precision, recall, and F1-score values of 98.78%, 97.2% and 97.98%, respectively
Zhou et al. [43]	ML	Propose a GAN-based unsupervised anomaly detection system	Yahoo Webscope	Case study	Outperform other state of arts systems with AUC and AP of 94% and 91%, respectively

retain important features of the original time series even in the case of a significant dimensionality reduction. de Souza et al. [22] propose a reference architecture that, based on the types of data, selects the algorithm which has the best performance and proceeds with the anomaly detection tasks. Feremans et al. [23] present an anomaly detection system based on the idea of identifying and merging patterns through the use of late integration. In particular, it selects a subset of patterns by computing an anomaly score, obtained by applying distance metrics, and then goes ahead with the anomaly detection phase. This technique consists in the extraction of patterns from sliding windows of time series separately, and then takes the union of the resulting patterns, so that each pattern is associated to one time series item. Bosman et al. [24] describe an approach leveraging neighborhood information. The work starts with the analysis of the possible aggregation metrics and metrics to find the correlation between these data, shows the maximum number of neighbors which leads to the best performance, and demonstrates that considering a number of neighbors higher than 5 or 6 leads to a drop in performance. Moshtaghi et al. [25] introduce a clustering algorithm based on guard zone to protect normal clusters and a state tracker to avoid the usage of a user-defined threshold to

Table 7
Articles about real-time models.

Author	Method used	Description	Experimental dataset	Validation techniques	Findings
Karim et al. [44]	DL	Propose to adapt existing univariate algorithms to the multivariate cases by modeling problems as tensors	Custom	Empirical	It outperforms most of the state of art algorithms
Ahmad et al. [45]	ML	Propose an algorithm that consider real-time constraints	NAB	Case study	It is able to detect spatial and temporal anomalies in predictable and noisy domains. It achieves a NAB score of 70% and outperforms similar methods
Laptev et al. [46]	ML	Propose a general and scalable anomaly detection framework	Yahoo Webscope	Case study	Thanks to several algorithms it automatically adapts to a lot of scenarios; always outperforms other frameworks, achieving a F1-score value of 75%
Chen et al. [47]	DL	Propose a Transformer-based framework capable of automatically learning a graph structure and a convolution algorithm to model information flow	SWaT, WADI, MSL, SMAP	Empirical, Case study	Outperforms other state of art algorithms with a recall of 91% and 84% on the selected datasets
Melnyk et al. [48]	ML	Propose a framework based on Semi-Markov switching autoregressive model	Custom	Empirical, Case study	It may be used in combination with other state of art frameworks to identify other important information. It achieves an AUC value from 88 to 95% for synthetic data and of 95% for real-world data
Lee and Kim [49]	ML	Propose a system based on the combinations of SARIMA and STL models to detect anomalies	NAB	Case study	It has better performance than LSTM in conventional time series analysis
Ren et al. [50]	DL	Propose a framework that combine Spectral Residual and CNN	KPI, Yahoo Webscope, Microsoft dataset	Case study	Outperforms other baseline solutions with F1-score values of 70%, 65%, and 54% on the three datsets considered
González et al. [51]	DL	Propose a model based on RNN and GAN	CPS, SYN-NET	Empirical	It shows promising performance: the discriminator detects 56% and the generator detects 70% of the whole attacks number
Karim et al. [52]	DL	Propose an evolution of Fully Convolutional Neural Networks (FCNs) by using an LSTM layer	UCR	Case study	Its performance achieves state of art algorithms with a precision rate ranging from 80% to 100%
Que et al. [53]	DL	Propose a 2-stage approach, using a fine-tuned autoencoder and a stacked LSTM	Yahoo Webscope	Empirical	The authors also propose a time-series-buffer to avoid redundant calculations and reduce system latency
Lee et al. [54]	DL	Propose a real-time anomaly detection for streaming data	Custom	Empirical	The model requires no training data or manual interventions. After a short probation period it starts the detection, achieving an F1-score value of 68%
Chen et al. [55]	DL	Propose an unsupervised framework based on sliding-window convolutional variational autoencoder	Custom	Empirical	It may detect temporal and spatial anomalies and not need additive sensor information or domain information. It achieves an F1-score value of 88% and a PRAUC value of 90%
Wang et al. [56]	ML	Propose an anomaly detection method based on multiple random convolution kernel and robust random cut forest	UCR	Empirical	It does not require training data and reaches values of precision, recall, and F1-score ranging from 90% to 93%
Ding et al. [57]	DL	Propose framework based on Hierarchical Temporal Memory and Bayesian Networks	NAB	Empirical	The combination with Bayesian Networks further improve HTM-based systems; it achieves 70% of accuracy with respect to 60% of previous models
Shen et al. [58]	DL	Propose a Temporal Hierarchical One-Class (THOC) network. Capture temporal dynamics by using a dilated recurrent neural network with skip connections	Power demand, SWaT, MSL, SMAP	Empirical	Outperforms other baseline methods with 63%, 45%, 98% and 88% of F1-score on the different datasets
Nanduri and Sherry [59]	DL	Propose a framework based on RNN-LSTM and GRU	Custom	Case study	Outperforms Multiple Kernel Anomaly Detection algorithms with a precision of 80% and an F1-score of 90%
Saurav et al. [60]	DL	Propose a temporal model based on RNN to detect variations in normal behavior	NAB, Yahoo Webscope	Empirical	It may adapt to change in frequency

Table 8
Articles about general anomaly detection.

Author	Method used	Description	Experimental dataset	Validation techniques	Findings
Hamamoto et al. [61]	ML	Propose a method based on Digital Signature of Network Segment using Flow Analysis	Custom	Empirical	The method does not require labeled data and achieve a ROC curve value of 99%
Maciąg et al. [62]	DL	Adapt OeSNN algorithm to anomaly detection task	NAB, Yahoo Webscope	Empirical	The algorithm's performance is not always the highest but metrics values range in a certain acceptable interval
Du et al. [63]	DL	Propose a framework based on Bi-LSTM network layer with temporal attention based mechanism	Beijing PM25, Power consumption, Italian air quality, Highways traffic	Empirical	The framework may jointly learn long-term dependencies and non-linear correlation features; achieves the lowest values of RMSE and MAE
Mohamudally and Peermamode-Mohaboob [64]	–	Outline several challenge to consider in anomaly detection engine building	–	Empirical	Outline the possible method to build an anomaly detection engine
Li et al. [65]	ML	Propose a clustering-based approach to detect both shape and amplitude anomalies	MIT-BIH Arrythmia	Empirical	The approach does not require labeled data; it helps to manage huge amount of data
Liu et al. [66]	DL	Propose several neural network methods to manage time series	Custom	Case study	RNN-AE are optimal with point anomalies and achieve 99% of AUC value; instead LSTM-ED are optimal with contextual anomalies and achieve 80% of AUC value
Hallac et al. [67]	ML	Propose a new method of model-based clustering (Toeplitz Inverse Covariance-based Clustering)	Custom	Empirical	Segments and cluster data breaking down high-dimensional time series into a clear sequential timeline
Gao et al. [68]	DL	Propose a framework based on time series decomposition and CNN	Yahoo Webscope	Case study	It achieves high performance and high efficiency with F1-score values of 90%
Kao and Jiang [69]	Statistical	Propose a framework for stationary and periodic time series	NAB	Empirical	The framework outperforms related methods
Guo et al. [70]	DL	Propose a framework based on GRU-gated and Gaussian Mixture VAE	Intel Berkeley Research Lab, Yahoo Webscope	Empirical	The framework outperforms other state of arts methods with a precision, recall, and f1-score values of 90%, 80% and 70%
Li and Jiang [71]	Statistical	Propose a framework for non-stationary and non-periodic time series	NAB	Empirical	Achieves better recall and F1-score than other methods
He et al. [72]	DL	Propose an attention based convolutional recurrent neural network framework	SWaT	Empirical	It may outperform popular deep neural network methods in term of MSE and MAE
Jain et al. [73]	ML	Propose a framework that reduces the number of feature considered for constraint environments	UCI	Empirical, Case study	The reduced feature model work with pre-processed data respect to the other. It reaches values of precision, recall and f1-score of 99%, 70% and 97%
Tadayon and Iwashita [74]	DL	Propose several neural network architecture to forecast time series	Custom	Empirical	Distance-based solutions outperform feature-based ones in most of the architecture, but feature-based methods are faster

decide if to create or not a new cluster for the data. This algorithm exploits the correlation between data points in time to cluster data, while maintaining a set of decision boundaries to identify noisy or anomalous data. Li et al. [26] leverage a GAN-based architecture for accomplishing anomaly detection, by considering an RNN-LSTM layer both in the Generator and in the Discriminator to manage multivariate time series. Experiments show that the authors achieve the best performance on multivariate time series analysis rather than on univariate time series, even considering the total number of features or a reduced number of them as input. Su et al. [27] propose a system based on a stochastic recurrent neural network that, through latent space, tries to reduce data dimensionality and is also capable of detecting which sliding windows contain the anomalous data. At the moment, this model combines an offline training phase, and an online detection phase but the authors plan to make online both of the phases. Takeishi and Yairi [28] propose a solution where they first extract features through sparse coding techniques and then, apply LSA (Latent Semantic Analysis) to reduce dimensionality. Zhang et al. [29] use the GRU model to reduce dimensionality and propose a dual-window method designed to detect and identify the eventual anomalies. Hyndman et al. [30] propose a model that combines PCA and alfa-hull to reduce feature space dimensions: they achieve that by considering only the first two components instead of all of them.

All the papers mentioned above use ML and DL techniques: in most of the cases DL approach gives a better performance with respect to ML, but it is also true that DL techniques suffer from some latency due to the training phase and this method requires also more data for training. As stated in Table 5, many authors work on empirical cases and only a few on real-cases scenario. Works on empirical models achieve very high performance and use a variety of methods such as clustering techniques, RNN, and GRU techniques. However, information about the actual performance of these models in a real-case scenario is not provided. Differently, Zhang et al. [29] propose a model based on a GRU

algorithm for detecting and identifying the eventual anomalies, and also reach very high performance. In particular, this model considers an inner window that contains the temporal feature of short periods of time series and an outer window that corresponds to a set of inner windows. If an anomaly occurs, the model is able to identify the inner window in which the anomaly happened. A GRU-based model to extract the temporal patterns and a CNN auto-encoder to locate anomalies according to both temporal and spatial features are used. Even in this case, an offline training phase is followed by an online detection phase. However, the authors validate this tool in a real scenario.

Dimensionality reduction open challenges: select data into IoT applications avoiding loss of useful information; identify the right metrics to include all the information in the decision process; improve parameter tuning phase to achieve better performance.

5.2. Anomaly localization

This subsection discusses anomaly localization techniques resumed in Table 6. Ding et al. [31] proposed a framework that analyzes data and, based on a health factor, decides if a further investigation is needed. In particular, the framework leverages a Gaussian Mixture Model to deal with multivariate time series, but it is a bit computationally expensive; to solve this issue the authors introduce a health factor to decide whether further analyses are needed or not. Kim and Cho [32] designed a system that extracts spatial and temporal features from data using a CNN and an LSTM network respectively, and finally use a DNN for classification. This system is characterized by an initial delay due to the pre-processing phase. Zhang et al. [33] construct multi-scale signature matrices to characterize sensors information and, given these matrices, an attention-based Convolution Long Short-Term Memory is used to extract temporal patterns and identify anomalies. Wang et al. [34] start with the generation of the symbolic cluster representation of the various windows and group them into the same cluster if they match the same rule. Then, there is a self-parameter tuning in which they make some hypotheses about data windows, and finally, they proceed with the anomaly detection phase. Wen and Keyes [35] adapt the U-Net algorithm to the case of anomaly detection and propose a framework based on the idea of transfer learning. Giannoni et al. [36] evaluate several algorithms and discover that the Local Density Cluster-based Outlier factor allows to achieve the best performance. Such a factor, can be used for both univariate and multivariate time series. The model of He et al. [37] uses a ResNet to capture temporal features, then learns the Granger Causal Graph and finally performs a time series regression to identify and locate anomalies. Goh et al. [38] used CUSUM techniques to identify anomalies: each data point gets a score associated and it is considered anomalous if its score is under a Lower Control Limit or above an Upper Control Limit. Yasaei et al. [39] proposed a sensor association algorithm that first generates sensor fingerprints, then clusters them and finally extracts the context of the systems. In particular, the base idea for the association algorithm is that sensors affected by the same event follow a similar pattern in their fingerprints. Subsequently, they split the generated fingerprint into small cub sections and cluster them. After this procedure is done, they get the so-called history vector which can be used to cluster future sensors. In addition, there is also a consensus mechanism to identify the source of the anomalies. Munir et al. [40] proposed a general framework capable of detecting all the three types of anomalies in an unsupervised way. He et al. [41] presented a model based on GAT (Graph Attention Network) which can identify and locate anomalies thanks to a correlation map. Hsieh et al. [42] employed a voting system to decide about the anomaly of data, and transfer learning to similar behavior systems to reduce the amount of data used for training and/or for testing. Stemming from [10,32] added another sliding window for a better feature selection. Zhou et al. [43] proposed a GAN-based system to detect and locate anomalies.

Even in the context of anomaly localization, we observe the usage of either ML or DL models, but this time DL models are used in the majority of the cases, due to their advantage over the ML ones, such as the better performance and the possibility to use them with large amounts of data. Most of the proposed models adopt RNN-LSTM, CNN, and other clustering techniques. There is always the aspect related to the empirical or case study validation, which often explains why the proposed methods achieve high performance. For example, Wang et al. [34] propose a system that starts with a dynamic clustering of time series sub-sequences identified by sliding windows, and then associate them with the right cluster according to certain rules. The rules are based on the idea that all the identified temporary clusters that match the same rules are allocated into the same final cluster. They also develop a self-parameter tuning in which they may merge or split some identified sliding windows based on the similarity between the data included in these windows. This example is not only relevant for its ability to localize anomalies and address, in some way, the tuning problem, but also for the fact that it has been tested on real case scenarios, showing that the proposed approach could work in real-world situations.

Anomaly localization open challenges: extend approaches to high dimensional scenarios; investigate the right size of sliding windows to avoid bad classification issues; increase the number of anomalies that the models can locate.

5.3. Real-time models

This subsection deals with real-time systems. The results of inspected papers are summarized in Table 7. Karim et al. [44] model each time series as a tensor, simplifying their representation. Ahmad et al. [45] propose an HTM (Hierarchical Temporal Memory) based system, which handles high-order sequences by using a composition of the current input and the context information from the previous ones. Laptev et al. [46] propose and evaluate several algorithms to manage various kinds of anomalies; their model is used at Yahoo Lab. Chen et al. [47] propose a framework in which the core idea is a learning graph structure, which is called the connection learning policy and is based on the Gumbal-softmax sampling strategy to learn bi-directional associations among sensors directly. They afford anomaly detection problems by defining a graph convolution algorithm, called Influence Propagation Convolution, concerning each specific node and its neighborhoods by applying a node-wise symmetric aggregation operation on the difference between nodes associated with all the edges emanating from each node. Melnyk et al. [48] propose a model that computes an anomaly score as the standard deviation of the output of the comparison between the prediction and the real data distribution. Lee and Kim [49] propose a framework based on SARIMA and STL that outperforms other solutions but requires more data for training. Ren et al. [50] propose the use of an SR (Spectral Residual) to extract useful information from time series and a CNN layer to detect anomalies. González et al. [51] propose a GAN model in which the generator applies an inverting search on the latent space and produces a residual loss; instead, the discriminator produces a discrimination loss

when deciding if the data came from the real data or the generator. Karim et al. [52] propose a refinement technique, that is similar to the transfer learning technique, which successfully tries to improve the performance of pre-trained models. Que et al. [53] propose a TS-buffer to avoid redundant calculation of LSTM gate operation and reduce systems latency. Lee et al. [54] propose a framework which learns by itself the data distribution and dynamically determines thresholds to adapt to pattern change. Chen et al. [55] train offline a model with historic data and then use it as an online detector. Wang et al. [56] propose a framework based on Multiple random convolution kernels to extract feature maps and RRCF (Robust Random Cut Forest) to detect anomalies; the RRCF is defined as the sum of the depths of all leaf nodes in the tree of each point of a set of data, and the anomaly score is the expected reduction in the complexity of the deletion of the node. Ding et al. [57] combine HTM model and Bayesian networks. They feed HTM model with time series, obtain a sparse code representation and compute the anomaly score based on the reconstruction error; this reconstruction error is used to compute the health factor. Relying on the value of this factor the model decides whether there is the need for further analysis or not. Shen et al. [58] extract temporal information and then fuse them with a Temporal Hierarchical network and a clustering algorithm. Nanduri and Sherry [59] propose a combination of RNN and GRU models and show that, after several tuning operations, the final models outperform the MKAD framework. Saurav et al. [60] propose a model which uses large prediction errors to detect anomalous behavior and is capable of adapting itself to data distribution change. After this brief description of the several models analyzed in this section, we list some papers that use real-case scenarios. Ahmad et al. [45] propose a system capable to detect spatial and temporal anomalies in a predictable and noisy domain. Melnyk et al. [48] propose a model that can be used in combination with other state-of-the-art frameworks to identify additional information. It achieves higher performance with real data rather than synthetic data. Ren et al. [50] propose the use of an SR (Spectral Residual) to extract useful information from time series and a CNN layer to detect anomalies. It reaches a 70% of F1-score. Nanduri and Sherry [59] evaluate the combination of RNN and GRU models, and reaches a precision of 80%.

As it is clear from observing the summary in Table 7, DL methods are the most used and the majority of them use LSTM models. In addition, we found that only a few approaches make use of advanced data representation schemas, such as binary vectors and graphs, while, in most cases, no particular data preprocessing steps are applied, and the analysis is performed by processing almost raw data. Indeed, data preprocessing might be computationally expensive and not very suited when time constraints are strict.

Real-time models open challenges: extend the same techniques applied to univariate time series also to multivariate time series; reduce FPR (False Positive Rate) in self-adaptive models to achieve better performance.

5.4. General anomaly detection

This subsection examines general anomaly detection frameworks, while Table 8 provides a synoptic resume of the studies falling in this topic. Hamamoto et al. [61] propose a hybrid approach that combines signature- and behavior-based models; they use a genetic algorithm to generate the DSNSF (Digital Signature of Network Segment using Flow Analysis) and Fuzzy logic to detect anomalies. For the fuzzification procedure they use a Gaussian Membership function which produces some values and then aggregates them; if this value exceeds a threshold, the model considers it as an anomaly, otherwise not. Maciąg et al. [62] adapt the OeSNN algorithm to the anomaly detection problem, identifying an input as anomalous if none of the output neurons fires or if the error between input and prediction is greater than the average prediction error. Du et al. [63] use Bi-LSTM network to learn time series hidden representation and extract hidden temporal features to construct latent space variables (temporal attention context vector) and an attention-based mechanism that selects the best encoder frames to use for anomaly detection. Mohamudally and Peermamode-Mohaboob [64] describe theoretically the most relevant aspects when designing an anomaly detection engine. Li et al. [65] use an extended version of Fuzzy C-Means that is capable of evaluating the impact of each variable on the clustering process. In particular, the model focuses on amplitude and shape anomalies; to reach the optimal impact of each variable they use a PSO (Particles Swarm Optimization) algorithm, based on a fitness function, in which each particle stores its best location visited. The available structure of multivariate time series is presented by using revealed clusters and centers, and partition matrix (FCM output) corresponding to optimal weights. Liu et al. [66] state that autoencoder achieves the best performance with point anomalies and, instead, LSTM-ED achieves the best performance with contextual anomalies. Hallac et al. [67] use MRF (Markov Random Field) to characterize the interdependences between different observations in a subsequence of a cluster. The authors define each cluster as a dependency network and show the relationship between the different sensors in short subsequences. Looking at a specific cluster, we can see how the various signal from various sensors can influence events at different time steps; in the MRF an edge represents a partial correlation between two variables. Gao et al. [68] combine the advantages of time series decomposition and CNN to handle the lack of sufficient labels and complicated patterns. Kao and Jiang [69] focus on stationary and periodic time series anomalies. Guo et al. [70] generate the reconstruction probability of the whole dataset and, on this value, detect anomalies. In particular, after the model training, they generate a list of reconstruction probability of each corresponding training data. When loading the training dataset, each sample is fed into an encoder to get the mean and deviation vector, and the system chooses a subset of these metrics, that are then sampled as a Gaussian distribution to generate L samples for every time series. This is fed to a decoder to obtain the reconstructed mean and the deviation vector. Finally, they compute the mean of all L and get the final reconstruction probability. Li and Jiang [71] focus on non-periodic and non-stationary time series anomalies. He et al. [72] enrich features interdependencies, then the inter-correlations in the time series are encoded by a neural network, and the temporal patterns are captured by an attention-based GRU network. Jain et al. [73] apply the PCA method to identify the first two components and detect anomalies using the Isolation Forest model. In particular, the model trained on the feature-reduced dataset achieves better performance than the model trained on the whole dataset, but it is affected by an initial system latency due to this pre-processing phase. Tadayon and Iwashita [74] compare distance and feature-based models; the result shows that DTW outperforms the feature-based clustering in most architecture but feature-based clustering methods outperform DTW in terms of speed and time complexity and still improve the forecasting accuracy significantly when they are compared to no clustering case. Table 8 shows that ML and DL models have been both used and it seems there is no preference

for any of them. We point out that [66,73] also consider the real-case scenario.

General anomaly detection open challenges: develop models that recognize time series structure at a high level of abstraction and address overhead problems with the distance metrics.

5.5. Characterization of used datasets

A crucial aspect of this research stream is the dataset used to validate the proposed solutions. This is an issue of crucial importance, as, the external validity strongly depends on the extent the samples represent the real world. Even after that, other features of the used data need to be checked, as well as data quality or data distributions. As stated in our review, it seems that almost all researchers tested the developed models on real-world datasets. These datasets are, sometimes, difficult to find as publicly available, as claimed by Fahim and Sillitti [7]. During our review, we have identified some public access, private and custom datasets.

NAB[5] (Numenta Anomaly Benchmark) is a publicly available streaming anomaly detection benchmark, released by Numenta in 2015. This dataset contains streaming data from different domains including road traffic, network utilization, online advertisements, and internet traffic. NAB repository contains six categories of datasets, both artificial and real, each of which has multiple CSV data files. Each CSV data file consists of two-time series, one of them being a series of timestamp values and the second one being a series of input values. The number of input values in data files varies between 1000 and 22 000, and overall there are 58 data files in the whole dataset. All the time series in the NAB repository are imbalanced, with less than 10%, on average, of time series input values being anomalies [62]. In its current version, the data file are distinguished into the following six categories:

- *artificialNoAnomaly*: contains artificially generated data files without anomalies;
- *artificialWithAnomalies*: contains data files which consist of artificial data with anomalies;
- *realAdExchange*: contains data files with online advertisements click recordings;
- *realKnownCauses*: contains data files such as hourly registered taxi schedules in New York City or CPU utilization;
- *realTraffic*: contains data files with freeway traffic recordings such as speed or travel time;
- *realTweets*: contains data files with Twitter volume statistics.

Only data files in *artificialNoAnomaly* category do not contain anomalies. The data files in the remaining categories contain at least one anomaly window; each anomaly window consists of multiple input values, and each data file can have several anomaly windows. Data are labeled either based on the known root cause of an anomaly or as a result of a pre-defined labeling procedure. Each data file consists of a timestamp and actual data values. Anomaly labels of each data file are given in a separate set of files. Although NAB provides a diverse labeled streaming anomaly detection dataset, there are few challenges that make it hard to be employed as a practical anomaly detection benchmark. Each data point with a ground truth anomaly label is centered by a defined anomaly window (10% of the length of a data file), which makes the ground-truth label of a normal data point also anomalous. This kind of labeling helps in calculating a good NAB score and leaves the recall very low. NAB score is introduced to reward early anomaly detection and penalize later detection based on the true and false detection within an anomaly window.

UCI[6] is a public collection of databases, domain theories, and data generators that are used by the machine learning community for the empirical analysis of machine learning algorithms. The archive was created as a ftp archive in 1987 by Davis Aha and fellow graduate students at UC Irvine. Since that time, it has been widely used by students, educators, and researchers all over the world as a primary source of machine learning datasets. The current version of the website has been designed in 2007 by Arthur Asuncion and David Newman. UC has some datasets with multivariate and univariate time series, and others that are instead useful for classification and clustering tasks. This dataset contains real and synthetic data collected over the years since 2007; some of them have a relatively high number of instances but, for some of them, some values are missing.

MSL[7] (Mars Science Laboratory) is a public dataset released by NASA and contains data from Curiosity rover from 2012. It includes 27 instances with an anomaly ratio of 10%. Three times a year, new datasets, especially relevant for the geosciences, are released by the Geoscience Node, that is one of the several discipline-specific nodes that make up the PSD (Planetary Data Systems).

SMAP[8] (Soil Moisture Active Passive) is a dataset released in 2015 also by NASA; it includes 55 instances with an anomaly ratio of 13%. It is divided into several levels related to spatial resolution and temporal coverage of the data in the dataset. The Level1 products contain raw or calibrated and geolocated instrument measurements from the SMAP Radar and Radiometer; they all have a temporal resolution of 49 min, the length of time required for SMAP satellite to complete a half orbit of the Earth. The Level2 products contain soil moisture retrievals derived from Level1 products and ancillary files, and they have a temporal resolution of 49 min. The Level3 products are daily composites of the Level2 soil moisture and freeze/thaw state data. The Level4 products provide model-derived root-zone soil moisture and carbon net ecosystem exchange.

SMD[9] (Server Machine Dataset) is a new 5-week-long dataset collected from a large Internet company; it includes 28 instances with an anomaly ratio of 4%. This labeled dataset contains three groups of entities. SMD is made up of data from 28 different machines, which are freely accessible by anyone who requires these data. It contains real and synthetic time series and/or sensors data.

The private datasets should be also mentioned, which are accessible after requesting them.

Yahoo Webscope[10] is released by Yahoo Labs. This dataset contains 367 real and synthetic time series with point anomaly labels. Each time series contains 1420–1680 instances. This anomaly detection benchmark is further divided into four sub-benchmarks namely A1, A2, A3, and A4 Benchmarks. A1 Benchmark contains 67 data files with real input time series values. Both single anomalous values and windows of anomalies occur in the data files. Each data file consists of three-time series: timestamps, input values, and a label for each input value (either anomalous or not). A2 Benchmark consists of 100 synthetic data files, which contain anomalies in the form of single anomalous values. Most input time series values in the category have their periodicity. As for A1 Benchmark, each data file contains only three-time series: timestamps, input values, and labels indicating the presence or

5 https://numenta.com/.

6 https://archive.ics.uci.edu/ml/datasets.php.

7 https://pds-geosciences.wustl.edu/missions/msl/.

8 https://nsidc.org/data/smap/smap-data.html.

9 https://sites.google.com/site/dilipprasad/home/singapore-maritime-dataset.

10 https://webscope.sandbox.yahoo.com/.

absence of anomalies. A3 Benchmark has 100 synthetic data files with anomalies in the form of single anomalous values. In comparison to A2 Benchmark, input values time series in the category are noisier. In addition to three standard time series (timestamps, input values, and anomalies labels), data files in this category also contain other time series (trend, noise, seasonality, and change point). A4 Benchmark contains 100 synthetic data files with anomalies. The majority of the anomalies correspond to sudden transitions from an input data trend to another significantly different input data trend.

SWaT[11] (Secure Water Treatment) is a private dataset, collected from a water treatment testbed for cyber-attack investigation launched in 2016. The dataset collection process lasted for a 11 days with the system operating 24 h per day. Various cyber-attacks were implemented on the testbed with different intents and divergent lasting durations (from a few minutes to an hour) in the final four days. The system was either allowed to reach its normal operating state before another attack was launched or the attacks were launched consecutively. The dataset present the following characteristics:

- Different attacks may last for different time windows due to different scenarios. Some attacks do not even take effect immediately. The system stabilization duration also varies across attacks. Simpler attacks, such as those aiming at changing flow rates, require less time for the system to stabilize while attacks that cause strong effects on the dynamics of system will require more time for stabilization;
- Attacks on one sensor (or actuator) may affect the performance on other sensors (or actuators), usually after a certain time delay;
- Similar types of sensors (or actuators) tend to respond to attacks in a similar way.

WADI[12] (Water Distribution) is another private dataset, collected from a water distribution testbed as an extension of the SWaT testbed. It consists of a total of 16 days of continuous operations, with 14 days under regular operation and 2 days with attack scenarios. The entire testbed contains 123 sensors and actuators.

Finally, we have custom datasets. These are created from public or private datasets, by applying some change to the data distribution or to the original dataset.

6. Discussion

This section summarizes all the issues identified during this review. The scientific production significantly increased in 2019, after a slow increment, while the absolute numbers show that the interest to the community is still limited even if growing. The majority of the papers have been published in conferences and journals, quite equally distributed, demonstrating that the topic is of interest to the community. Empirical studies are adopted by most papers, providing results that are statistically significant. The approaches make use of machine learning in the largest part, even if in the newest papers the deep learning starts to appear, and it is reasonable to expect that it will be much more employed in future research. As stated in Section 3 and according to Fahim and Sillitti [7] there are still some open issues in the literature so far:

- limited or difficult access to data;
- systems are trained on normal data and abnormal ones are scarce;
- data are often noisy;
- too many parameters to handle;
- no studies on data fusion techniques;
- no studies on ensemble learning that could reduce false positive rate.

As reported in Section 5, we observed some open issues and challenges related to the specific identified topics. Specifically, in Section 5.1, we observe the lack of comprehensive solutions to (i) select IoT applications data avoiding loss of useful information, (ii) identify the right metrics for including all the crucial information in the decision process, and (iii) improve parameter tuning phase for achieving the highest performance as possible. To address these limitations, some authors tried to introduce new techniques, many of them attempted to adapt existing ones, while others explored the possibility of using neighbor nodes information.

In a similar fashion, Section 5.2 raises several open issues, such as (i) extending approaches to high dimensional scenarios, (ii) investigating the right size of sliding windows to avoid bad classification, and (iii) increasing the number and types of anomalies the systems are able to locate. In this context, the authors investigated different solutions, such as (i) representing the whole structure as a graph, (ii) generating sensor fingerprints, (iii) using voting systems to decide if there is an anomaly or not and also to locate them, but general solutions to address these issues are still missing.

In Section 5.3 further challenges emerge, such as (i) extending the same techniques applied to univariate time series also to multivariate time series, and (ii) the need to reduce FPR (False Positive Rate) to achieve better performances. To deal with these issues, some authors used graph convolution algorithms, some others introduced a way of remembering the computation already done avoiding useless computation, and others tried to apply a transfer learning approach to reduce the need for data. In addition, Section 5.4 identifies issues with some systems that do not recognize time series structure when dealing with very high order time series due to the possibility that the optimization method falls into a local optima and problems due to the overhead entailed by the distance metric selected. To address these limitations some authors tried to introduce new techniques, while the majority of them attempted to adapt existing ones. For each of the identified topics, much research has been done; most of the authors achieve high performance with their models but due to the limitations identified in this review further investigation is still necessary.

Concerning the datasets, most of the authors prefer to use public or free accessible ones, because of the limited or difficult access to data, while some others use only private datasets, or private datasets in combination with the public and free accessible ones to further test their solutions. Only a few authors, instead, use neither public nor private datasets. In particular, these authors prefer customizing the dataset by stemming from a private or a public one and applying some changes to obtain new datasets with additive information. In this context, frameworks for assessing the quality of synthetic and real-world data collections would be very useful. Finally, another direction that needs further investigation and shows potential in this field of research is the development and the application of new or existing data fusion techniques.

7. Conclusions

Given the growing interest in the Internet of Things (IoT) paradigms, in this paper, we surveyed the main models, frameworks, and solutions proposed in the scientific literature to perform

11 https://itrust.sutd.edu.sg/itrust-labs_datasets.
12 https://itrust.sutd.edu.sg/itrust-labs_datasets.

anomaly detection in IoT environments. More specifically, our systematic literature review considered the studies on anomaly detection in IoT time-series data and highlighted the specific challenges concerning topics such as dimensionality reduction, localization of anomalies, real-time monitoring, and datasets usage. In summary, the main findings achieved in our systematic review are as follows:

- need for advanced techniques for reducing the dimensionality of the data collected by IoT devices;
- shortage of methods for performing anomaly localization in high dimensional scenarios;
- lack of robust universal approaches and techniques for real-time anomaly detection;
- lack of general contextual anomaly detection systems using time series;
- the few available datasets very often contain synthetic data likely leading to incomplete assessments.

Considering the specific open issues highlighted, we believe that further research in the directions identified in this paper is crucial for advancing knowledge in the area of anomaly detection, in general, and for gradually improving the reliability of IoT systems, in particular. In the future, we plan to explore ways to deal with some of the open challenges highlighted in our work. In particular, we want to conceive approaches for contextual anomaly detection based on IoT multivariate time-series in high-dimensional dynamic scenarios. More specifically, we aim at investigating both standard and custom approaches enabling time-series dimensionality reduction for efficient anomaly localization in real-time contexts.

CRediT authorship contribution statement

Arnaldo Sgueglia: Methodology, Investigation, Validation, Visualization, Data curation, Writing – original draft, Writing – review & editing. **Andrea Di Sorbo:** Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing. **Corrado Aaron Visaggio:** Conceptualization, Methodology, Investigation, Visualization, Writing – original draft, Writing – review & editing. **Gerardo Canfora:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors gratefully thank Paolo Campegiani and the people at the Bit4id company for providing suggestions and feedback useful to improve the paper's structure and contents.

References

[1] L. Farhan, S.T. Shukur, A.E. Alissa, M. Alrweg, U. Raza, R. Kharel, A survey on the challenges and opportunities of the Internet of Things (IoT), in: 2017 Eleventh International Conference on Sensing Technology (ICST), IEEE, 2017, pp. 1–5.

[2] A. Di Mauro, A. Di Nardo, G.F. Santonastaso, S. Venticinque, An IoT system for monitoring and data collection of residential water end-use consumption, in: 28th International Conference on Computer Communication and Networks, ICCCN 2019, Valencia, Spain, July 29 - August 1, 2019, 2019, pp. 1–6.

[3] A. Čolaković, M. Hadžialić, Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, Comput. Netw. 144 (2018) 17–39.

[4] Y. Ma, J. Rao, W. Hu, X. Meng, X. Han, Y. Zhang, Y. Chai, C. Liu, An efficient index for massive IOT data in cloud environment, in: 21st ACM International Conference on Information and Knowledge Management, CIKM'12, Maui, HI, USA, October 29 - November 02, 2012, 2012, pp. 2129–2133.

[5] M. Canizo, A. Conde, S. Charramendieta, R. Miñón, R.G. Cid-Fuentes, E. Onieva, Implementation of a large-scale platform for cyber-physical system real-time monitoring, IEEE Access 7 (2019) 52455–52466.

[6] A.A. Cook, G. Mısırlı, Z. Fan, Anomaly detection for IoT time-series data: A survey, IEEE Internet Things J. 7 (7) (2019) 6481–6494.

[7] M. Fahim, A. Sillitti, Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review, IEEE Access 7 (2019) 81664–81681.

[8] J. Azar, A. Makhoul, R. Couturier, J. Demerjian, Robust IoT time series classification with data compression and deep learning, Neurocomputing 398 (2020) 222–234.

[9] Y. Zhu, M. Imamura, D. Nikovski, E. Keogh, Introducing time series chains: a new primitive for time series data mining, Knowl. Inf. Syst. 60 (2) (2019) 1135–1161.

[10] C. Yin, S. Zhang, J. Wang, N.N. Xiong, Anomaly detection based on convolutional recurrent autoencoder for IoT time series, IEEE Trans. Syst. Man Cybern.: Syst. (2020).

[11] J. Li, S. Di, Y. Shen, L. Chen, FluxEV: a fast and effective unsupervised framework for time-series anomaly detection, in: Proceedings of the 14th ACM International Conference on Web Search and Data Mining, 2021, pp. 824–832.

[12] I.V. Farahani, A. Chien, R.E. King, M.G. Kay, B. Klenz, Time series anomaly detection from a Markov chain perspective, in: 2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, 2019, pp. 1000–1007.

[13] F. Demrozi, G. Pravadelli, A. Bihorac, P. Rashidi, Human activity recognition using inertial, physiological and environmental sensors: A comprehensive survey, IEEE Access 8 (2020) 210816–210836.

[14] A. Fakhrazari, H. Vakilzadian, A survey on time series data mining, in: 2017 IEEE International Conference on Electro Information Technology (EIT), IEEE, 2017, pp. 476–481.

[15] M. Ali, A. Alqahtani, M.W. Jones, X. Xie, Clustering and classification for time series data in visual analytics: A survey, IEEE Access 7 (2019) 181314–181338.

[16] A. Gaddam, T. Wilkin, M. Angelova, Anomaly detection models for detecting sensor faults and outliers in the iot-a survey, in: 2019 13th International Conference on Sensing Technology (ICST), IEEE, 2019, pp. 1–6.

[17] B. Sharma, L. Sharma, C. Lal, Anomaly detection techniques using deep learning in iot: A survey, in: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), IEEE, 2019, pp. 146–149.

[18] R.K. Dwivedi, A.K. Rai, R. Kumar, Outlier detection in wireless sensor networks using machine learning techniques: a survey, in: 2020 International Conference on Electrical and Electronics Engineering (ICE3), IEEE, 2020, pp. 316–321.

[19] S. Keele, et al., Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report, Citeseer, 2007.

[20] O. Köksal, B. Tekinerdogan, Obstacles in data distribution service middleware: a systematic review, Future Gener. Comput. Syst. 68 (2017) 191–210.

[21] M. Krawczak, G. Szkatuła, An approach to dimensionality reduction in time series, Inform. Sci. 260 (2014) 15–36.

[22] P.S.S. de Souza, F.P. Rubin, R. Hohemberger, T.C. Ferreto, A.F. Lorenzon, M.C. Luizelli, F.D. Rossi, Detecting abnormal sensors via machine learning: An IoT farming WSN-based architecture case study, Measurement 164 (2020) 108042.

[23] L. Feremans, V. Vercruyssen, B. Cule, W. Meert, B. Goethals, Pattern-based anomaly detection in mixed-type time series, in: Machine Learning and Knowledge Discovery in Databases, Springer, Cham, 2020, pp. 240–256.

[24] H.H. Bosman, G. Iacca, A. Tejada, H.J. Wörtche, A. Liotta, Spatial anomaly detection in sensor networks using neighborhood information, Inf. Fusion 33 (2017) 41–56.

[25] M. Moshtaghi, C. Leckie, J.C. Bezdek, Online clustering of multivariate time-series, in: Proceedings of the 2016 SIAM International Conference on Data Mining, SIAM, 2016, pp. 360–368.

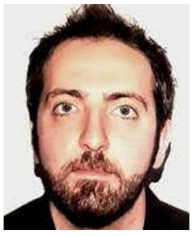
[26] D. Li, D. Chen, J. Goh, S.-k. Ng, Anomaly detection with generative adversarial networks for multivariate time series, 2018, arXiv preprint arXiv:1809.04758.

[27] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, D. Pei, Robust anomaly detection for multivariate time series through stochastic recurrent neural network, in: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019, pp. 2828–2837.

[28] N. Takeishi, T. Yairi, Anomaly detection from multivariate time-series with sparse representation, in: 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2014, pp. 2651–2656.

[29] S. Zhang, X. Chen, J. Chen, Q. Jiang, H. Huang, Anomaly detection of periodic multivariate time series under high acquisition frequency scene in IoT, in: 2020 International Conference on Data Mining Workshops (ICDMW), IEEE, 2020, pp. 543–552.
[30] R.J. Hyndman, E. Wang, N. Laptev, Large-scale unusual time series detection, in: 2015 IEEE International Conference on Data Mining Workshop (ICDMW), IEEE, 2015, pp. 1616–1619.
[31] N. Ding, H. Ma, H. Gao, Y. Ma, G. Tan, Real-time anomaly detection based on long short-Term memory and Gaussian Mixture Model, Comput. Electr. Eng. 79 (2019) 106458.
[32] T.-Y. Kim, S.-B. Cho, Web traffic anomaly detection using C-LSTM neural networks, Expert Syst. Appl. 106 (2018) 66–76.
[33] C. Zhang, D. Song, Y. Chen, X. Feng, C. Lumezanu, W. Cheng, J. Ni, B. Zong, H. Chen, N.V. Chawla, A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data, in: Proceedings of the AAAI Conference on Artificial Intelligence, 2019, pp. 1409–1416.
[34] X. Wang, J. Lin, N. Patel, M. Braun, A self-learning and online algorithm for time series anomaly detection, with application in CPU manufacturing, in: Proceedings of the 25th ACM International on Conference on Information and Knowledge Management, 2016, pp. 1823–1832.
[35] T. Wen, R. Keyes, Time series anomaly detection using convolutional neural networks and transfer learning, 2019, arXiv preprint arXiv:1905.13628.
[36] F. Giannoni, M. Mancini, F. Marinelli, Anomaly detection models for IoT time series data, 2018, arXiv preprint arXiv:1812.00890.
[37] S. He, H. Huang, S. Yoo, W. Yan, F. Xue, T. Wang, C. Xu, Flight data anomaly detection and diagnosis with variable association change, in: Proceedings of the 36th Annual ACM Symposium on Applied Computing, 2021, pp. 346–354.
[38] J. Goh, S. Adepu, M. Tan, Z.S. Lee, Anomaly detection in cyber physical systems using recurrent neural networks, in: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), IEEE, 2017, pp. 140–145.
[39] R. Yasaei, F. Hernandez, M.A. 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), IEEE, 2020, pp. 1–9.
[40] M. Munir, S.A. Siddiqui, A. Dengel, S. Ahmed, DeepAnT: A deep learning approach for unsupervised anomaly detection in time series, IEEE Access 7 (2018) 1991–2005.
[41] Q. He, Y. Zheng, C. Zhang, H. Wang, MTAD-TF: Multivariate time series anomaly detection using the combination of temporal pattern and feature pattern, Complexity 2020 (2020).
[42] R.-J. Hsieh, J. Chou, C.-H. Ho, Unsupervised online anomaly detection on multivariate sensing time series data for smart manufacturing, in: 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), IEEE, 2019, pp. 90–97.
[43] B. Zhou, S. Liu, B. Hooi, X. Cheng, J. Ye, BeatGAN: Anomalous rhythm detection using adversarially generated time series, in: IJCAI, 2019, pp. 4433–4439.
[44] F. Karim, S. Majumdar, H. Darabi, S. Harford, Multivariate LSTM-FCNs for time series classification, Neural Netw. 116 (2019) 237–245.
[45] S. Ahmad, A. Lavin, S. Purdy, Z. Agha, Unsupervised real-time anomaly detection for streaming data, Neurocomputing 262 (2017) 134–147.
[46] N. Laptev, S. Amizadeh, I. Flint, Generic and scalable framework for automated time-series anomaly detection, in: Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2015, pp. 1939–1947.
[47] Z. Chen, D. Chen, Z. Yuan, X. Cheng, X. Zhang, Learning graph structures with transformer for multivariate time series anomaly detection in IoT, 2021, arXiv preprint arXiv:2104.03466.
[48] I. Melnyk, A. Banerjee, B. Matthews, N. Oza, Semi-Markov switching vector autoregressive model-based anomaly detection in aviation systems, in: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 1065–1074.
[49] S. Lee, H.K. Kim, Adsas: Comprehensive real-time anomaly detection system, in: International Workshop on Information Security Applications, Springer, 2018, pp. 29–41.
[50] H. Ren, B. Xu, Y. Wang, C. Yi, C. Huang, X. Kou, T. Xing, M. Yang, J. Tong, Q. Zhang, Time-series anomaly detection service at microsoft, in: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019, pp. 3009–3017.
[51] G.G. González, P. Casas, A. Fernández, G. Gómez, On the usage of generative models for network anomaly detection in multivariate time-series, 2020, arXiv preprint arXiv:2010.08286.
[52] F. Karim, S. Majumdar, H. Darabi, S. Chen, LSTM fully convolutional networks for time series classification, IEEE Access 6 (2017) 1662–1669.
[53] Z. Que, Y. Liu, C. Guo, X. Niu, Y. Zhu, W. Luk, Real-time anomaly detection for flight testing using AutoEncoder and LSTM, in: 2019 International Conference on Field-Programmable Technology (ICFPT), IEEE, 2019, pp. 379–382.
[54] M.-C. Lee, J.-C. Lin, E.G. Gan, ReRe: A lightweight real-time ready-to-go anomaly detection approach for time series, in: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE, 2020, pp. 322–327.
[55] T. Chen, X. Liu, B. Xia, W. Wang, Y. Lai, Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder, IEEE Access 8 (2020) 47072–47081.
[56] Q. Wang, B. Yan, H. Su, H. Zheng, Anomaly detection for time series data stream, in: 2021 IEEE 6th International Conference on Big Data Analytics (ICBDA), IEEE, 2021, pp. 118–122.
[57] N. Ding, H. Gao, H. Bu, H. Ma, H. Si, Multivariate-time-series-driven real-time anomaly detection based on bayesian network, Sensors 18 (10) (2018) 3367.
[58] L. Shen, Z. Li, J. Kwok, Timeseries anomaly detection using temporal hierarchical one-class network, Adv. Neural Inf. Process. Syst. 33 (2020) 13016–13026.
[59] A. Nanduri, L. Sherry, Anomaly detection in aircraft data using recurrent neural networks (RNN), in: 2016 Integrated Communications Navigation and Surveillance (ICNS), Ieee, 2016, pp. 5C2–1.
[60] S. Saurav, P. Malhotra, V. TV, N. Gugulothu, L. Vig, P. Agarwal, G. Shroff, Online anomaly detection with concept drift adaptation using recurrent neural networks, in: Proceedings of the Acm India Joint International Conference on Data Science and Management of Data, 2018, pp. 78–87.
[61] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrão, M.L. Proença Jr., Network anomaly detection system using genetic algorithm and fuzzy logic, Expert Syst. Appl. 92 (2018) 390–402.
[62] P.S. Maciąg, M. Kryszkiewicz, R. Bembenik, J.L. Lobo, J. Del Ser, Unsupervised anomaly detection in stream data with online evolving spiking neural networks, Neural Netw. 139 (2021) 118–139.
[63] S. Du, T. Li, Y. Yang, S.-J. Horng, Multivariate time series forecasting via attention-based encoder–decoder framework, Neurocomputing 388 (2020) 269–279.
[64] N. Mohamudally, M. Peermamode-Mohaboob, Building an anomaly detection engine (ADE) for Iot smart applications, Procedia Comput. Sci. 134 (2018) 10–17.
[65] J. Li, H. Izakian, W. Pedrycz, I. Jamal, Clustering-based anomaly detection in multivariate time series data, Appl. Soft Comput. 100 (2021) 106919.
[66] Y. Liu, Z. Pang, M. Karlsson, S. Gong, Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control, Build. Environ. 183 (2020) 107212.
[67] D. Hallac, S. Vare, S. Boyd, J. Leskovec, Toeplitz inverse covariance-based clustering of multivariate time series data, in: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.
[68] J. Gao, X. Song, Q. Wen, P. Wang, L. Sun, H. Xu, RobustTAD: Robust time series anomaly detection via decomposition and convolutional neural networks, 2020, arXiv preprint arXiv:2002.09545.
[69] J.-B. Kao, J.-R. Jiang, Anomaly detection for univariate time series with statistics and deep learning, in: 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), IEEE, 2019, pp. 404–407.
[70] Y. Guo, T. Ji, Q. Wang, L. Yu, G. Min, P. Li, Unsupervised anomaly detection in IoT systems for smart cities, IEEE Trans. Netw. Sci. Eng. 7 (4) (2020) 2231–2242.
[71] Y.-L. Li, J.-R. Jiang, Anomaly detection for non-stationary and non-periodic univariate time series, in: 2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), IEEE, 2020, pp. 177–179.
[72] J. He, M. Dong, S. Bi, W. Zhao, X. Liao, A deep neural network for anomaly detection and forecasting for multivariate time series in smart city, in: 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), IEEE, 2019, pp. 615–620.
[73] P. Jain, S. Jain, O.R. Zaïane, A. Srivastava, Anomaly detection in resource constrained environments with streaming data, IEEE Trans. Emerg. Top. Comput. Intell. (2021).
[74] M. Tadayon, Y. Iwashita, A clustering approach to time series forecasting using neural networks: A comparative study on distance-based vs. feature-based clustering methods, 2020, arXiv preprint arXiv:2001.09547.

Arnaldo Sgueglia is a Ph.D. student in Software Engineering at the Department of Engineering of the University of Sannio, Italy. He obtained B.Sc. in Computer Engineering from University of Sannio, Italy, in 2017, while, in 2020, he received M.Sc. in Computer Engineering from the same university. His research interests include IoT security and applications.



Andrea Di Sorbo is a research fellow at the University of Sannio, Italy. He received his Ph.D. in information technology from the University of Sannio in 2018, followed by a postdoctoral fellowship at the same University. He serves and has served as guest editor for Frontiers in Big Data, Information and Software Technology, and Science of Computer Programming journals, as a reviewer for software engineering journals (TSE, EMSE, JSS, IST, SCP, JSEP). and as a program committee member of relevant international conferences (ICSE, ASE, ARES, MOBILESoft, SEAA). His research interests include software maintenance and evolution, empirical software engineering, and software security and privacy.

Corrado Aaron Visaggio is an associate professor of CyberSecurity at University of Sannio. He is chair of the node of University of Sannio for the CINI National Cyber Security Lab. He is the scientific coordinator of several projects funded by firms operating in CyberSecurity, concerning malware analysis, vulnerability assessment, and data protection. He serves in the Editorial Board of the International Journal of Computer Virology and Frontiers in Big Data, and in several Program Committees (MALWARE, ARES, SECRYPT, SEKE, ITASEC, FoRSE, DATA, Hufo, MobiSys, WETSoM, ISSRE). His research interests are: malware analysis, data privacy and protection, software security, empirical software engineering.

Gerardo Canfora is a professor of computer science at the School of Engineering of the University of Sannio, Italy. He serves on the program and organizing committees of a number of international conferences. He was general chair of WCRE06 and CSMR03, and program cochair of ICSE15, WETSoM12 and 10, ICSM01 and 07, IWPSE05, CSMR04 and IWPC97. He is co-editor of the journal of Software: Evolution and Processes. Canfora authored 200 research papers; his research interests include software maintenance and evolution, security and privacy, empirical software engineering, and services-oriented computing.