Intelligent Systems with Applications 18 (2023) 200232

Contents lists available at ScienceDirect

Intelligent Systems with Applications

journal homepage: www.journals.elsevier.com/intelligent-systems-with-applications

Review

Anomaly classification in industrial Internet of things: A review

Martha Rodríguez [a], Diana P. Tobón [b], Danny Múnera [a,*]

[a] Universidad de Antioquia, Medellin, Colombia
[b] Universidad de Medellín, Medellín, Colombia

ARTICLE INFO

Keywords:
Industrial Internet of things
IIoT
Anomaly detection
Anomaly classification
Context-awareness
Context-information

ABSTRACT

The fourth industrial revolution (Industry 4.0) has the potential to provide real-time, secure, and autonomous manufacturing environments. The Industrial Internet of Things (IIoT) is a powerful tool to make this promise a reality because it can provide enhanced wireless connectivity for data collection and processing in interconnected plants. Implementing IIoT systems entails using heterogeneous technologies, which collect incomplete, unstructured, redundant, and noisy data. This condition raises security flaws and data collection issues that affect the data quality of the systems. One effective way to identify poor-quality data is through anomaly detection systems, which provide specific information that helps to decide whether a device is malfunctioning, a critical event is occurring, or the system's security is being breached. Using early anomaly detection mechanisms prevents the IIoT system from being influenced by anomalies in decision-making. Identifying the origin of the anomaly (e.g., event, failure, or attack) supports the user in making effective decisions about handling the data or identifying the device that exhibits abnormal behavior. However, implementing anomaly detection systems is not easy since various factors must be defined, such as what method to use for the best performance. What information must we process to detect and classify anomalies? Which devices have to be monitored to detect anomalies? Which device of the IIoT system will be in charge of executing the anomaly detection algorithm? Hence, in this paper, we performed a state-of-the-art review, including 99 different articles aiming to identify the answer of various authors to these questions. We also highlighted works on IIoT anomaly detection and classification, used methods, and open challenges. We found that automatic anomaly classification in IIoT is an open research topic, and additional information from the context of the application is rarely used to facilitate anomaly detection.

1. Introduction

Internet of Things (IoT) is a paradigm in system design that supplies connectivity to devices to provide intelligent services to system users Botta et al. (2016). Industrial Internet of Things (IIoT) applies this paradigm to industrial systems Younan et al. (2020). It opens the scene to intelligent applications that benefit the development of industrial processes Wang et al. (2021a), from monitoring or remote control applications to early detection of faults or anomalies in the system operation Wang et al. (2020b). In this context, anomalies are data collected or generated by IIoT devices whose magnitude deviates from the expected or predictable value Saurav et al. (2018). Anomalous data can indicate that a system is wasting resources, a critical situation occurs in a process, or a device exhibits abnormal behavior Fahim and Sillitti (2019). Failures, events, or attacks cause these abnormal values DeMedeiros et al. (2023), Ghosh et al. (2019), Karkouch et al. (2016). Failures are data generated by faulty or poorly calibrated devices; events are external phenomena, incidents, or changes in the application context; attacks, in turn, usually breach one or several nodes in the IIoT network, compromising the entire system security. Hence, these anomalies must be identified and treated to avoid affecting the quality of decisions Karkouch et al. (2016).

Early detection of anomalies in an industrial process is crucial to implement decisions based on real-time information, thus reducing maintenance costs, minimizing machine downtime, increasing safety, and improving product quality Wang et al. (2020b). Different types of anomalies have been widely studied separately. However, since they coexist in industrial processes, it is necessary to distinguish between them (e.g., event, failure, and attack) to reduce consequences, accelerating the attention by addressing the qualified staff in charge to attend each specific type of anomaly Tertytchny et al. (2020). For example,

* Corresponding author.
E-mail addresses: mlucia.rodriguez@udea.edu.co (M. Rodríguez), dtobon@udemedellin.edu.co (D.P. Tobón), danny.munera@udea.edu.co (D. Múnera).
URLs: https://www.udea.edu.co (M. Rodríguez), https://www.udemedellin.edu.co (D.P. Tobón), https://www.udea.edu.co (D. Múnera).

https://doi.org/10.1016/j.iswa.2023.200232
Received 9 September 2022; Received in revised form 25 April 2023; Accepted 7 May 2023
Available online 12 May 2023

events can affect product quality and, therefore, must be handled by the production department; failures can lead to process stoppage or cause significant damage to machinery. Thus maintenance staff must handle these anomalies. Thus, knowing the anomaly source helps to choose the right recovery actions to minimize abnormal behavior Tertytchny et al. (2020). In contrast, attacks can lead to loss of confidentiality, privacy, or integrity of the information and even a system malfunction. The Information Technology (IT) department usually handles these attacks.

However, building a model capable of classifying IIoT anomalies is challenging because data are highly unbalanced; data describing an anomaly are scarce compared to data related to normal behaviors Sun et al. (2020). In addition, predictions must be accurate to avoid false alarms, misinterpretations, or overlooking some abnormal behavior. Likely, the person who must attend to an abnormal event differs from the person who solves a fault or an attack. If the anomaly detection system only warns of abnormal behavior without determining its origin, additional time and data will be needed to diagnose the anomaly's cause manually. Manual diagnosis of the source of an anomaly implies that some people have access to confidential data for determining whether the anomaly is an event, a failure, or an attack Langone et al. (2020). Human intervention will be necessary to decide who is in charge and how to resolve this situation Tertytchny et al. (2020). In contrast, automatic anomaly classification methods restrict the number of personnel in contact with critical information from the manufacturing process, thus facilitating knowledge protection in digital transformation environments with multi-organizational collaborative networks Langone et al. (2020).

Differentiating an anomaly's source without additional device data is a complex problem. Nevertheless, IIoT offers an opportunity to have redundant application contextual data Moradbeikie et al. (2020). One strategy to improve automatic anomaly classification is precisely using context information. Alexopoulos et al. (2018) define context as any information that characterizes the situation of an entity (i.e., person, place, or object). For example, channel or traffic characteristics, quality of service, environmental data, vibration signals, sound recordings, or power consumption patterns may be considered contextual information Angelopoulos et al. (2020), Anton et al. (2017), Gai et al. (2017). Some techniques for anomaly classification only consider data content information (data collected from a system to ensure its routine operation) without considering the application context. Context awareness can help detect spatial, sequential, and temporal correlations between devices; as data become increasingly complex, the importance of using context in anomaly classification increases. Sensors could deliver, besides measured variables, data that characterize a device's spatial or temporal location Hayes and Capretz (2014); thus, context information allows us to understand the detection methods with unbalanced data better Sun et al. (2020).

Anomaly classification uses pattern recognition by extracting statistical information based on prior knowledge. When an anomaly does not have a distinct signature, it is detected indirectly because of unusual manifested behavior; context information helps train probabilistic models for detecting and classifying these anomalies Ehsani-Besheli and Zarandi (2017). Therefore, context-based anomaly classification is helpful in dynamically changing systems Ehsani-Besheli and Zarandi (2017).

In this work, we performed a review of the state-of-the-art in anomaly detection and classification, thus identifying what is being done to classify the origin of anomalies and how context information helps to achieve this goal. The main contribution of this paper can be summarized as follows,

- We performed a literature review to identify works on IIoT anomaly detection and classification using statistical, machine learning (ML), and deep learning (DL) methods.
- We found that most of the research in this field focuses on detecting malicious attacks or anomalies in general. In addition, research that classifies detected anomalies is rare.
- We identified some open research topics, such as IIoT anomaly classification and the incorporation of contextual information in those solutions. We identified the level of implementation of the methods studied by determining the layer of the IIoT system in charge of executing the algorithm.
- We analyzed the use of context information in anomaly detection systems considering that several authors have highlighted the benefit of its use, as it facilitates the detection of spatial and temporal correlation between variables.

This paper is organized as follows. Section 2 discusses related works and justifies the need for this literature review. Then, in Section 3, some main concepts that will guide the work are defined. Section 5 describes the methodology research and criteria used to analyze the different scientific papers selected. Subsequently, Section 5 shows the obtained results according to information classification criteria. Finally, we highlighted the open challenges for future research and conclusion in Sections 6 and 7, respectively.

2. Related works

In this section, we describe different review papers on anomaly detection in industrial environments found in the literature as shown in Table 1. De et al. (2022) review deep generative models (DGM) used in IIoT. DGM combines the flexibility of deep learning with the inference power of probabilistic modeling. The authors identify challenges, opportunities, and potential research directions in anomaly detection, trust boundary protection, network traffic prediction, and platform monitoring.

In their systematic mapping, Aranda et al. (2022) study context awareness, edge computing, data analysis, and IIoT in smart grids. They review some papers that propose machine-learning solutions for anomaly detection in smart grids. Fahim and Sillitti (2019) present a systematic literature review of abnormal behavior prediction techniques in IoT. The authors analyzed statistical and machine-learning methods to identify abnormal behavior in intelligent inhabitant environments, transportation systems, health care systems, smart objects, and industrial systems. They found research gaps in data collection, analysis of unbalanced data sets, and a few research papers on anomaly detection in real scenarios. Authors in DeMedeiros et al. (2023), in turn, describe how anomaly detection is being performed on Internet of Things and sensor networks. They classify anomaly causes as a malicious attack, sensor fault, and significant environmental change registered as an abnormal state by the sensor. Still, they need to expand on this idea during the report. Also, this survey describes some public datasets used to test the anomaly classifiers.

Authors in Angelopoulos et al. (2020) focus on ML-based solutions to fault detection, prediction, and prevention in Industry 4.0. They examine various cloud/fog/edge industrial architectures and their data collection and threat detection implications. In Alruwaili (2021), authors study intrusion detection and prevention in IIoT and compare different mechanisms used to detect, prevent, and protect IIoT systems against various vulnerabilities, threats, and attacks. Finally, authors in Zeyu et al. (2020) review the security challenges of edge computing in the 5G context, which is a crucial technology to promote a large-scale deployment of edge computing. While all the reviewed papers in our research discuss anomaly detection results, none address the issue of classification of the origin of an anomaly. Hence, in this paper, we presented a state-of-the-art review on anomaly detection and classification, which identifies the use of contextual information on these systems.

3. Background

Different terms in the manufacturing industry have emerged to describe systems that collect data and decide to act on a physical process

Table 1
Related review works in anomaly detection.

Reference	Year	Short description	Context-aware	Anomaly detection	Anomaly classification
DeMedeiros et al. (2023)	2023	Anomaly detection on the Internet of Things and sensor networks,	✗	✓	✗
Aranda et al. (2022)	2022	Context-aware edge computing and IoT in smart grids	✓	✓	✗
De et al. (2022)	2022	Deep generative models in IIoT	✗	✓	✗
Alruwaili (2021)	2021	Intrusion detection and prevention in Industrial IoT	✗	✓	✗
Zeyu et al. (2020)	2020	Edge Computing Security	✗	✓	✗
Fahim and Sillitti (2019)	2019	Anomaly detection, analysis and prediction techniques in IoT	✗	✓	✗
Angelopoulos et al. (2020)	2019	Tackling faults in the Industry 4.0	✗	✓	✗
This review	2023	Anomaly classification in IIoT	✓	✓	✓

through actuators, or to alert a human operator. Boyes et al. (2018) indicate that the most commonly used terms for these systems are Cyber-Physical Systems (CPS), Operational Technology (OT), and Industrial Control Systems (ICS). Authors also consider an overlap between Industry 4.0 and Industrial Internet concepts, which combines technologies such as the Internet of Things, cloud computing, and data analytics to transform business outcomes. Therefore, before describing how different authors detect IIoT anomalies, we considered it essential to define the main terms related to the problem we are addressing in this work, such as the Industrial Internet of Things, anomaly definition, and context information.

3.1. Industrial Internet of things

IIoT is a "smart objects network that uses generic information technologies and optional cloud or edge computing platforms, allowing them real-time, intelligent, and autonomous access, collection, analysis, communications within an industrial environment to optimize overall production value" Boyes et al. (2018). IIoT requires high-quality service related to determinism, latency, performance, availability, reliability, security, and privacy. It does not seek to replace field-level automation (i.e., sensors and actuators) but automates monitoring, optimization, and prediction tasks that people traditionally perform Sisinni et al. (2018). However, this level of connectivity causes some vulnerability effects to propagate throughout the industrial plant, where IIoT devices share common vulnerabilities with standard IoT devices Hansch et al. (2019).

Karkouch et al. (2016) describe some issues compromising data quality in IoT systems. Based on that work, we highlighted those aspects that apply to industrial settings. For example, communication between heterogeneous devices, limited processing and storage resources, intermittent connections and packet loss in IIoT wireless networks, and vandalism by disgruntled employees. Environmental conditions in industrial settings can affect device performance. Due to the manufacturing process, sensors may lack accuracy, damage from extreme environmental conditions, lack of calibration, or malfunctions. Another factor that can reduce data quality is exposure to electromagnetic noise from motors and transformers. On the other hand, cyber-attacks compromise data privacy, integrity, and availability, and faulty elements can generate outliers since they keep sending data. However, actions to ensure data privacy and processing could reduce data quality Karkouch et al. (2016).

3.2. Anomaly as event, attack, or failure

Saurav et al. (2018) define an anomaly as a behavior that is not normal. Authors in Ghosh et al. (2019) use the term outlier and describe it as an observation (or a subset) that appears inconsistent with the rest of the data set. Ghosh et al. (2019), in turn, define the terms event, failure, and attack.

- **Event**: It is a situation that changes the state of the real world, such as a natural phenomenon that alters some monitored variables Karkouch et al. (2016): This type of anomaly lasts longer than failures and changes the data pattern. It is hard to distinguish between event and fault because faulty sensors can also generate this error. Thus, spatial correlation is a crucial tool for detecting anomalies because data from faulty sensors lack spatial relationships, whereas data measurements from events do possess such relationships Ghosh et al. (2019).
- **Failure**. It refers to data coming from a faulty sensor measurement due to a lack of calibration or device malfunction Mohamudally and Peermamode-Mohaboob (2018). They occur because of an unexpected change in data and are different from the rest. These errors affect information quality and must be detected and removed before using data. Failures can be classified into two categories such as transient and permanent. The first type causes an element to fail for a specific time, generating random values, and the second causes a component to permanently malfunction and continuously send erroneous data Moradbeikie et al. (2020).
- **Attack**: A malicious attack compromises one or more nodes in an IIoT network, tricking others into interacting with them and compromising the entire network's security. Wireless communications are a primary channel for system intrusions Ghosh et al. (2019).

3.3. Context information

In our review, we differentiated content and context information to determine whether an anomaly originated from an event, a failure, or a malicious attack. For Alexopoulos et al. (2018), context is any information that characterizes the situation of an entity and its interaction with a context-aware application. In this work, we referred to content information as the data collected from a system to ensure its routine operation. Context information, in turn, is also defined as the additional data from an industrial approach to detect or classify anomalies. For example, in a water treatment plant, the tank's level and motor pump's power consumption can be content information, as these data are necessary to operate the system correctly. While surrounding temperature and sensor power consumption can be considered context information since these data are not required for the plant operation; instead, they can help determine whether an anomaly is an event, a failure, or an attack.

4. Methodology

This study focuses on understanding anomaly detection in IIoT and identifies available solutions to classify anomalies as events, failures, or attacks. Also, it is explored how context-aware information has been used to improve anomaly detection algorithms. To elaborate this review, we considered the guidelines for conducting systematic mapping studies in software engineering by Petersen et al. (2015).

Based on the Petersen guidelines, we defined the following review methodology. First, we stated a set of research questions from the main objective of this review. Second, a search query is created based on the research questions and applied to relevant databases. Third, the retrieved papers are filtered by using exclusion criteria. These criteria decide which articles were eligible and which were not. After reading the abstract, the authors decide whether the article is about "anomaly

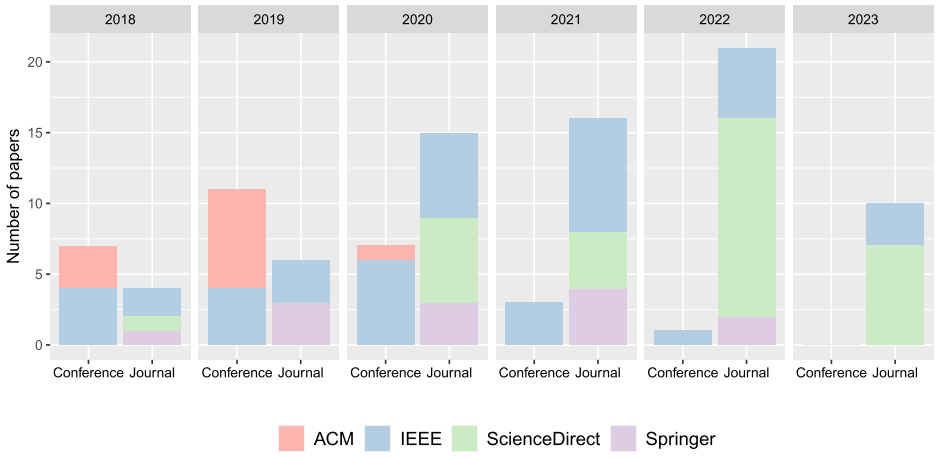

Fig. 1. Journals and conferences related to IIoT anomaly detection between 2018 and March 2023.

detection in IIoT". Finally, removing duplicate submissions is a manual process that identifies and eliminates duplicate copies of articles in different journal databases. Data obtained from this step is the basis for developing this review. Below, we explain each of the steps in detail.

4.1. Research questions

We have defined three research questions for our state-of-the-art analysis as described to follow,

- RQ1: Which techniques and methods enable detecting and classifying anomalies in IIoT?
- RQ2: What kind of validation do authors perform for proposed strategies?
- RQ3: How does context information improve anomaly detection in IIoT?

4.2. Search query and databases

We created the following search query by identifying the main keywords in the research question:

```
(("Industrial IoT" OR IIoT OR "Industrial Internet of Things") AND "anomaly detect*")
```

Then, this query was applied to four relevant databases in the field, such as Springer, Science Direct, ACM, and IEEE.

4.3. Exclusion criteria

We identified peer-reviewed and available online papers describing techniques or methods to detect anomalies in IIoT. Still, we excluded surveys, systematic reviews, mapping studies, editorials, prefaces, interviews, news, correspondences, discussions, comments, readers' letters, panel discussions, poster sessions, abstracts, or books.

4.4. Classification criteria

Following the defined methodology, we used the research questions to identify the criteria to extract information from the retrieved papers, as shown to follow,

- Criterion 1: Does the work detect events, failures, or attacks? This criterion indicates whether a work detects events, failures, attacks, or combinations. This information is extracted following the definition of an event, failure, and attack given in the background Section.
- Criterion 2: Does the work use statistical, machine learning, or deep learning methods to detect anomalies? The reviewed papers are divided into three groups: those that primarily use statistical methods to detect anomalies, those that use machine learning techniques, and those that specifically use deep learning.
- Criterion 3: Does the work diagnose anomaly origin as an event, failure, and attack? This criterion determines whether a strategy differentiates the anomaly's origin or not.
- Criterion 4: Does the work use context information? In this review, context information is additional data collected from an industrial process for anomaly detection. This criterion aims to identify whether a work uses this context information to implement the detection or classification algorithm.
- Criterion 5: Where does the work detect anomalies in the perception, network, or application layer? This criterion indicates whether a proposal detects anomalies occurring at the perception, network, or application layer of the IIoT system.
- Criterion 6: Which device runs the anomaly detection algorithm (node, edge, cloud, or local server)? Each type of device in the IIoT network has different constrained resources (e.g., storage, processing, and latency), which limits the possibility of implementing the model in real time.

5. Results and discussion

This section presents the results after we applied the above review methodology. Fig. 1 shows a summary of the reports found by year. After using the exclusion criteria, we selected 99 papers, of which 70 are journal papers (11 from Springer, 32 from ScienceDirect, and 27 from IEEE) and 29 conferences (11 from ACM and 18 from IEEE). From this figure, we noticed that the number of published papers has been growing continuously in the last few years, which indicates that this topic has attracted interest from the research community.

We also highlighted the techniques used by different authors to detect anomalies and identified if they detect anomalies in general or anomalies of a particular type, such as events, failures, or attacks. At the same time, we analyzed the use of contextual information for implementing anomaly detectors. Fig. 2 shows an overview of the results of this report, including the percentage of papers that meet each classification criterion. From the 99 articles reviewed, only 8% used information considered to be context-aware. Most reports (56.5%) implemented deep learning methods to detect anomalies. The anomaly detection is intended mainly for edge devices (48.9%), and the anomaly detection system is primarily executed on the edge computing (19%) layer. Finally, most papers (58.5%) do not mention where algorithms were implemented.

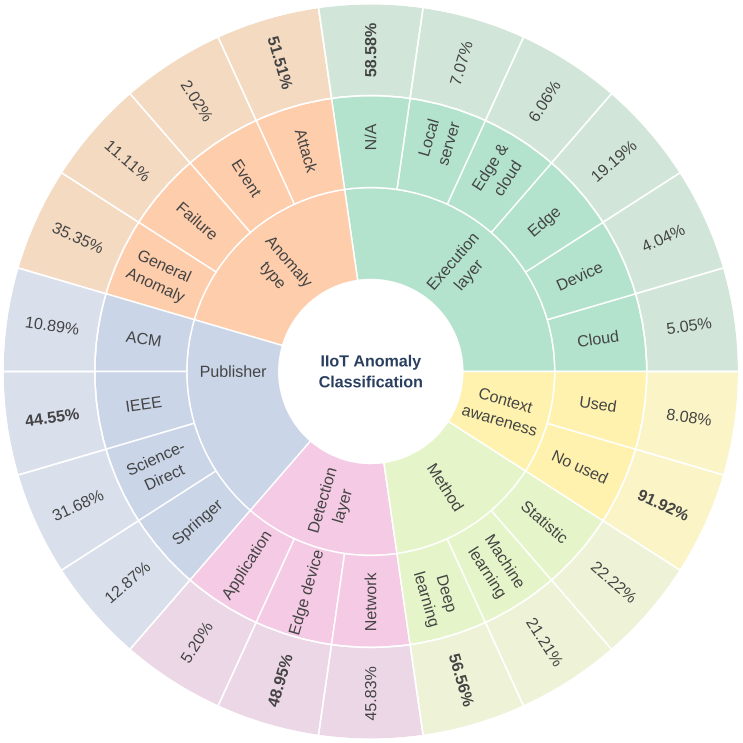

Fig. 2. Percentage of papers included in this state-of-the-art review that meet each classification criterion described in Section 5.1 (papers classification criteria).

Fig. 3. Histogram of papers performing anomaly detection classified by the detection method used and the type of anomaly detected.

To facilitate the detection of research trends, we grouped papers according to the anomaly detection methods used (i.e., statistical, machine learning, or deep learning). We determined if the reports studied use information that can be considered context-aware and in which device the proposed algorithms are executed (i.e., end device, edge, cloud, or local server). We identified if the proposed strategy detects events, failures, attacks, or a combination. We also analyzed which layer the anomaly detection mechanism is implemented (i.e., perception, network, or application). In the following, we present the data extracted from the papers, first analyzing the proposed anomaly detection mechanism and then classifying the source of the anomaly.

5.1. Anomaly detection

Table 2 presents the papers that detect general anomalies or events, failures, and attacks in particular. Attack detection receives the most attention from researchers in this field, followed by the detection of general anomalies.

Related to the RQ1, "Which techniques and methods make possible detecting and classifying anomalies in IIoT?", Fig. 3 shows the distribution of papers that detects anomalies classified by the detection method and the types of anomaly detected. We can see that most of the reports (56) use deep learning techniques to detect anomalies. It is worth mentioning that many authors combine statistical techniques with Machine Learning (ML) or Deep Learning (DL) methods. For example, before applying ML or DL method, some authors use Principal Component Analysis (PCA) to reduce the number of dimensions based on variable correlation De Vita et al. (2020b, 2021), Elnour et al. (2021), Kumar et al. (2022), Liu et al. (2019), Shi et al. (2019), Yang et al. (2022b).

Regarding the use of context information (RQ3), according to the definition given in the background section of this paper, Fig. 4 shows that the largest portion of papers (91 out 99) do not use context information, where the analysis is limited to only industrial process data. For instance, Hashmat et al. (2022) use a device traffic context identifier to extract information from the vulnerability identification engine. The proposal presented in Bodo et al. (2020) records sensing device specifications and environmental noise, while Demertzis et al. (2020) monitors the internal parameters of the device, such as operating temperature, battery status, and operating time. Similarly, in Raposo et al. (2019), authors use performance metrics, such as execution time, energy counter, and MCU cycles. In Garitano et al. (2019), different contextual information is gathered; they measure the time interval between incoming connections and packet size. The work presented in Shi et al. (2019) uses the power consumption of the IIoT device. Authors in Peng et al. (2019), in turn, collect geographically relevant and time-sensitive data, and authors in Ghaeini et al. (2018) include a sensor noise model for anomaly detection. The work developed by Hashmat et al. (2022) is the only one that uses the term "context", whereas that other works use "metadata" Garitano et al. (2019), "metrics" Raposo et al. (2019), or "features" Bodo et al. (2020), Demertzis et al. (2020).

Fig. 5 shows the layer where the algorithm is intended to detect anomalies. Most works extract data from the perception layer (47 out 99), the network layer (44 out 99), or both. A few methods (5) use data from the application layer to detect anomalies Peng et al. (2019), Wang et al. (2020b).

Regarding the RQ2, "What kind of validation do authors perform for proposed strategies?" we found that most of the works only show

Table 2
Type of detected anomaly.

Events	Failures	Attacks
Peng et al. (2019), Ouyang et al. (2018)	Ferrari et al. (2019), De Vita et al. (2020a), Liu et al. (2020a), De Vita et al. (2020b), Wang et al. (2020b), De Vita et al. (2021), Garmaroodi et al. (2020), Rousopoulou et al. (2022), Dzaferagic et al. (2021), Kim et al. (2023), Çavdar et al. (2023)	Garitano et al. (2019), Anton et al. (2019), Raposo et al. (2018), Li et al. (2020b), Liu et al. (2019), Bernieri et al. (2019b), Wang (2020), Al-Hawawreh and Sitnikova (2019), Bernieri and Pascucci (2019), Krundyshev and Kalinin (2019), Shi et al. (2019), Li et al. (2020a), Bae et al. (2018), Bernieri et al. (2019a), Gorbenko and Popov (2020), Garg et al. (2020), Enăchescu et al. (2019), Aoudi and Almgren (2020), Tandiya et al. (2018), Wang et al. (2021b), Huong et al. (2021), Zhang et al. (2020), Cui et al. (2021), Wang et al. (2021a), Hashmat et al. (2022), Khan et al. (2021), Mukherjee (2022), Elnour et al. (2021), Cai et al. (2021), Nedeljkovic and Jakovljevic (2022), Seo et al. (2021), Weinger et al. (2022), Su et al. (2022), Rey et al. (2022), Friha et al. (2022), Kumar et al. (2022), Liu et al. (2022), Yang et al. (2022a), Ghaeini et al. (2018), Zugasti et al. (2018), Muna et al. (2018), Schneider and Böttinger (2018), Madhawa et al. (2018), Chen et al. (2021), Wangwang et al. (2021), Kozik et al. (2021), Kumar et al. (2023), Wang et al. (2021c), Douiba et al. (2023), Halder and Newe (2023),
General Anomaly		
Raposo et al. (2019), Yang et al. (2020), Park et al. (2020), Razzak et al. (2020), Faisal et al. (2019), Wu et al. (2019), Bodo et al. (2020), He et al. (2020), Demertzis et al. (2020), Genge et al. (2019), Al-Hawawreh et al. (2019), Li et al. (2020c), Liu et al. (2020b), Kong et al. (2021), Zhan et al. (2021), Aruquipa and Diaz (2022), Ketonen and Blech (2021), Yang et al. (2022b), Liu et al. (2020a), Savic et al. (2021), Wu et al. (2021), Dang et al. (2021), Wang et al. (2022), Zhou et al. (2020), Kim et al. (2018), Saurav et al. (2018), Ba et al. (2022b), Ba et al. (2022a), Truong et al. (2022), Wang et al. (2022), Hu et al. (2022), Pan et al. (2022), Sankaran and Kim (2023), Feng et al. (2022), Nizam et al. (2022)		

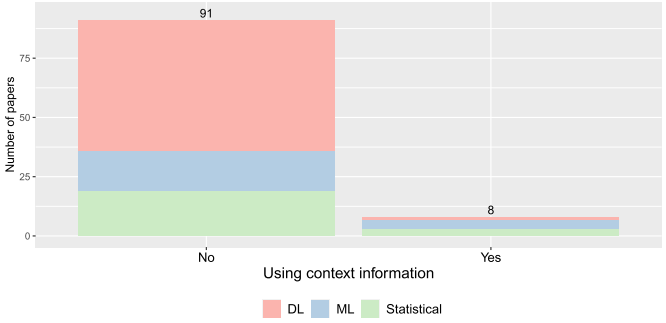

Fig. 4. Number of papers using context information grouped by the detection method.

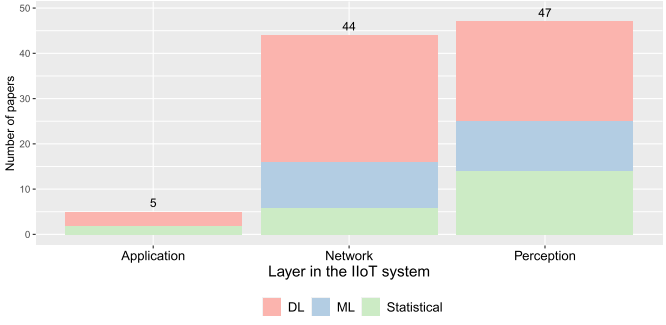

Fig. 5. Number of papers reporting the layer where the anomaly occurs.

the results of the offline training without reporting the performance of the online detection. Sometimes the layer where the algorithm is executed is reported. One of the papers reporting the online performance is Kumar et al. (2022), which proposes an IoT botnet detection solution running at a Raspberry Pi as an edge gateway. Huong et al. (2021) use a Raspberry PI in a federated learning approach to detect cyber-attacks. Authors in De Vita et al. (2020a) describe a platform for fault prediction with ML algorithms running on edge and cloud computing. In Demertzis et al. (2020), authors run a deep auto-encoder in the cloud and distribute a Blockchain on every device. Authors in De Vita et al. (2020b), in turn, use an edge gateway board to support humans in detecting mechanical anomalies in a real IIoT testbed (Fig. 6).

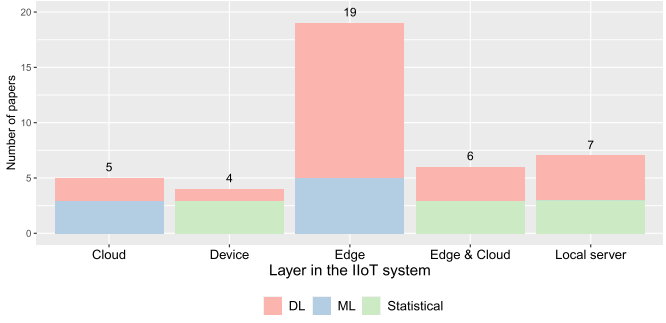

Fig. 6. Histogram of papers that reports the IoT layer used to execute the anomaly detection algorithm.

5.1.1. *Anomaly detection using statistical methods*

Various statistical methods have been applied to implement anomaly detection systems, such as phase-aware hidden semi-Markov model Cai et al. (2021), discrete wavelet transform Dang et al. (2021), fast Fourier transform De Vita et al. (2021), swap center metric Gorbenko and Popov (2020), singular spectrum analysis Aoudi and Almgren (2020), time series correlation with Pearson coefficient Li et al. (2020c), principal component analysis Garitano et al. (2019), Markov chains for discrete time Faisal et al. (2019), Genge et al. (2019), Bayesian dynamic equalization assigning reward and punishment mechanisms to IoT nodes Wang et al. (2020a), extended Kalman filter Bernieri and Pascucci (2019), deterministic finite automata Bernieri et al. (2019a), Dempster-Shafer's "Theory of Evidence" Çavdar et al. (2023), Enăchescu et al. (2019), linear dynamic state space models Ghaeini et al. (2018), and null space based on stochastic subspace identification methods Zugasti et al. (2018).

We reported the information extracted from the selected papers in three Tables with a similar format (Tables 3-5). The first column of each table shows the paper's reference, and the second column briefly describes the detection strategy. The column identified as *anomaly* specifies whether the report detects events, failures, attacks, or any abnormality. The *classify* column, in turn, indicates whether that research identifies anomaly sources. Based on the six criteria cited above, Table 3 summarizes the scientific papers using statistical methods to detect anomalies. The *context-awareness* column records report that use additional information (context information) taken from a process to detect anomalies, as well as the *detection layer* column indicates whether the

Table 3
Anomaly detection proposals using statistical methods (E stands for Events, F stands for Failures, and A stands for Attacks).

Reference	Anomaly detection strategy	Anomaly	Classify (E-F-A)	Context Aware	Detection Layer	Execute Layer
Hashmat et al. (2022)	Vulnerability signature formation engine	Attacks	✗	✓	Network	-
Aruquipa and Diaz (2022)	Bio inspired manufacturing with vibration sensors	All	✗	✗	Device	Device
Wang et al. (2022)	Correlation between time series through the self-attention mechanism	All	✗	✗	Device	-
Zhan et al. (2021)	Hierarchical representation for time series anomaly detection	All	✗	✗	Device	-
De Vita et al. (2021)	Semi-Supervised Bayesian Anomaly Detection	Failures	✗	✗	Device	Edge & Cloud
Cai et al. (2021)	Content-agnostic payload-based anomaly detector	Attacks	✗	✗	Network	-
Dang et al. (2021)	Discrete Wavelet Transform and Principal Component Analysis	All	✗	✗	Device	Local server
De Vita et al. (2020a)	On board fault prediction by analyzing real time sensor data	Failures	✗	✗	Device	Edge & Cloud
Gorbenko and Popov (2020)	Swap centre metric method	Attacks	✗	✗	Device	-
Aoudi and Almgren (2020)	Singular spectrum analysis	Attacks	✗	✗	Device	-
Li et al. (2020c)	Correlation between multivariate time series	All	✗	✗	Device	-
Garitano et al. (2019)	Monitoring incoming connection patterns on server side	Attacks	✗	✓	Network	Local server
Faisal et al. (2019)	Deep-packet inspection	All	✗	✗	Network	-
Wang (2020)	Dynamic Bayesian equalization	Attacks	✗	✗	Network	-
Bernieri and Pascucci (2019)	Extended Kalman Filter (EKF)	Attacks	✗	✗	Device	Device
Genge et al. (2019)	Hotelling's T2 statistics and the univariate cumulative sum	All	✗	✗	Device	-
Bernieri et al. (2019a)	Deterministic Finite Automata	Attacks	✗	✗	Network	-
Enăchescu et al. (2019)	Dempster-Shafer's "Theory of Evidence"	Attacks	✗	✗	Device	-
Peng et al. (2019)	Fuzzy theory	Events	✗	✓	Application	Edge & Cloud
Ghaeini et al. (2018)	Linear Dynamical State-space (LDS)	Attacks	✗	✗	Device	Local server
Zugasti et al. (2018)	Stochastic Subspace Identification	Attacks	✗	✗	Application	-
Madhawa et al. (2018)	Invariants are formulated by experts	Attacks	✗	✗	Device	Device

authors detect anomalies occurring in IIoT devices, networks, or application layers. Finally, the *execute layer* column shows where the authors proposed implementing the algorithm.

It can be seen from Table 3 that some authors detect anomalies of different origins but without classifying the type of anomaly. For example, Garitano et al. (2019) detect (man-in-the-middle) attacks, sensor failures, and communication problems by examining the contribution of each variable to an abnormal event. However, their proposal does not automatically detect the source of the anomaly, limiting the functionality to generate an alarm for a human operator who diagnoses whether it is a plant event, a communication event, or an attack. The authors include data from physical and network variables in their detection method, which could be considered context information, called "metadata".

Ghaeini et al. (2018) present an approach intended to detect any anomaly, although they focus only on malicious attack detection. While authors in Hashmat et al. (2022) propose an automated context-aware anomaly assessment rule-set framework based on vulnerability signatures. This method uses a cumulative sum of residuals on historical system data to detect stealthily changing variables, where noise patterns in sensors (e.g., sensor accuracy level or water movement in a tank) can be considered context information for this proposal.

5.1.2. Anomaly detection using machine learning techniques

We identified several machine learning methods used to detect anomalies, such as support vector machine Garmaroodi et al. (2020), Kumar et al. (2022), Razzak et al. (2020), Rousopoulou et al. (2022), k-nearest neighbors Shi et al. (2019), Yang et al. (2020), decision trees Ahakonye et al. (2023b), Bodo et al. (2020), Kumar et al. (2022), optimized gradient boosting decision tree Cui et al. (2021), Douiba et al. (2023), isolation forest Elnour et al. (2021), Yang et al. (2022b), and spatial density-based clustering of applications with noise Garg et al. (2020).

Table 4 summarizes information extracted from the papers using machine learning techniques to detect anomalies. This Table identifies several proposals that detect anomalies of different natures without diagnosing the origin. Authors in Raposo et al. (2019) use metrics from a specific microcontroller brand to detect firmware and hardware anomalies (buffer overflow attacks, SPI failures, voltage drops, and high-temperature failures). However, it assumes that attacks cause all anomalies. In this case, metrics delivered by the microcontroller unit (execution time, energy counter, microcontroller unit cycles) could be considered context information.

Bodo et al. (2020) use decision trees to determine whether data correspond to an anomaly. Although they do not determine the origin of an anomaly, this strategy could detect whether data are labeled appropriately. The authors use specifications from detection devices, environmental noise, and available processing resources to support detecting an anomaly, which could be considered context information.

Another work presented in Shi et al. (2019) uses the power consumption of an IoT device to detect anomalies. In this case, a device's power consumption could be considered context information. The report in He et al. (2020), in turn, identifies anomalies by comparing suspicious data, from a specific sensor, against data from other sensors recording similar variables. However, they do not determine whether it is a fault, an attack, or an event in the application context. On the other hand, authors in Ahakonye et al. (2023a), Douiba et al. (2023) classify the specific type of attack using decision trees.

5.1.3. Anomaly detection using deep neural networks

Neural networks are used in most papers for anomaly detection. The most common models used are Convolutional Neural Networks (CNN) Liu et al. (2022), Nedeljkovic and Jakovljevic (2022), Seo et al. (2021), Recurrent Neural Networks (RNN) Park et al. (2020), Wang et al. (2020b), bidirectional long and short-term memory (LSTM) Kong et al. (2021), Li et al. (2020a), Wang et al. (2021b), Wu et al. (2019), variational autoencoders Al-Hawawreh and Sitnikova (2019), Bernieri et al. (2019b), Huong et al. (2021), Savic et al. (2021), CNN-LSTM Liu et al. (2020b), Khan et al. (2021), Mukherjee (2022), and Transformers Ba et al. (2022b), Chen et al. (2021), Kim et al. (2023), Kozik et al. (2021), Kumar et al. (2022), Truong et al. (2022).

Table 5 presents papers proposing anomaly detection using Deep Learning techniques. Some works use neural networks as multilabel classifier Al-Hawawreh et al. (2019), Çavdar et al. (2023), Mukher-

Table 4
Anomaly detection proposals using machine learning methods (E stands for Events, F stands for Failures, and A stands for Attacks).

Reference	Anomaly detection strategy	Anomaly	Classify (E-F-A)	Context Aware	Detection Layer	Execute Layer
Ahakonye et al. (2023a)	Decision tree and Chi-square for feature selection	Attacks	✓*	✗	Network	-
Douiba et al. (2023)	Decision tree and gradient boosting	Attacks	✓*	✗	Network	Local server
Yang et al. (2022b)	Detect data distribution change in time and train the new model	All	✗	✗	Device	-
Rousopoulou et al. (2022)	Generic platform for anomaly detection	Failures	✗	✗	Device	Cloud
Su et al. (2022)	Machine-learning tree-based methods	Attacks	✗	✗	Network	-
Rey et al. (2022)	Autoencoder in federated learning	Attacks	✗	✗	Device	Edge
Kumar et al. (2022)	Botnet detection using network-edge traffic	Attacks	✗	✗	Network	Edge
Garmaroodi et al. (2020)	Data mining	Failures	✗	✗	Device	Edge
Cui et al. (2021)	Margin synthetic minority oversampling technique for unbalanced data	Attacks	✗	✗	Network	Edge
Elnour et al. (2021)	data-driven attack detection using Isolation Forest	Attacks	✗	✗	Device	-
Yang et al. (2020)	Secure vector homomorphic encryption scheme	All	✗	✗	Device	Cloud
Razzak et al. (2020)	Randomized nonlinear one-class support vector machine	All	✗	✗	Device	-
Bodo et al. (2020)	Feature selection method based on hierarchical feature ranking	All	✗	✓	Device	-
He et al. (2020)	Decision triggered data transmission and collection protocol	All	✗	✗	Device	-
Garg et al. (2020)	Density-Based Spatial Clustering of Applications with Noise (DBSCAN)	Attacks	✗	✗	Network	-
Zhang et al. (2020)	Maximum correlation minimum redundancy feature selection algorithm	Attacks	✗	✗	Network	-
Anton et al. (2019)	Matrix Profiles detect attacks that occur multiple times	Attacks	✗	✗	Network	-
Raposo et al. (2019)	Use on-node metrics available in hardware	All	✗	✓	Device	-
Raposo et al. (2018)	One Class Support Vector Machine	Attacks	✗	✓	Network	Edge
Shi et al. (2019)	Extract statistical and spectral features	Attacks	✗	✓	Network	-
Ouyang et al. (2018)	Multi-view learning based ensemble learning solution	Events	✗	✗	Device	Cloud

Methods marked with * classify anomalies but without identifying the three kinds of anomalies defined in this review.

jee (2022), Park et al. (2020), Sankaran and Kim (2023), Saurav et al. (2018), Wang et al. (2020a, 2020c). For example, authors in Çavdar et al. (2023) combine one-dimensional convolution neural networks and the Dempster–Shafer decision fusion method to detect and classify some specific failures types, and authors in Sankaran and Kim (2023) use a robust multi-cascaded convolutional neural networks (CNN) classification approach to distinguish between Sybil and DoS attacks. The deep neural network architecture developed by Mukherjee (2022) incorporates inherent convolutional neural networks, which act as a multi-label classifier to determine the intrusion points of attacks. The work presented in Dzaferagic et al. (2021) trains a multi-class fault classification auto-encoder using sensor measurements collected during faulty operation. The work presented in Wang et al. (2020b) uses RNN to detect anomalies and provides insights into the timestep at which an anomaly occurred. This system assists a human operator, which in turn, locates the source of a problem. Whereas authors in Çavdar et al. (2023), Sankaran and Kim (2023) classify the specific type of attack o failure, respectively.

Several authors tackle the issue of dealing with many features and data in an IoT context. Working with big data in real-time anomaly detection systems presents several challenges because of the constrained resources of memory and processing power of edge devices and the high latency of cloud computing processing. Regarding neural network models, some works use long short-term memory (LSTM) to leverage spatial and temporal correlation on abnormal detection Ferrari et al. (2019), Li et al. (2020a), Wu et al. (2019). Some results use Principal Components Analysis (PCA) to reduce the dimensions in a dataset before training a neural network De Vita et al. (2020b), Liu et al. (2019). Other papers use auto-encoder networks and only train models with normal operating data, which avoids dealing with rare anomalous data in an industrial system Kim et al. (2018), Muna et al. (2018), Schneider and Böttinger (2018).

Another solution to take advantage of IIoT characteristics is the federated learning technique, which is used for training and detecting anomalies in a distributed way Liu et al. (2020a), Wang et al. (2021a). In the last two years, modified versions of Transformer and the attention mechanism Vaswani et al. (2017) have gained momentum in the field of anomaly detection Ba et al. (2022b), Chen et al. (2021), Kim et al. (2023), Kozik et al. (2021), Kumar et al. (2022), Truong et al. (2022), some authors use graph-CNN for feature selection and transformers for anomaly detection Ba et al. (2022a, 2022b), Chen et al. (2021), other works use auto-encoders based on transformers for the same task Truong et al. (2022), Wang et al. (2022). In addition, transfer learning with a variational graph auto-encoder is used in a trajectory anomaly detection strategy Hu et al. (2022). Proposals in this section neither perform automatic classification of the anomaly origin as an event, attack, or failure nor identify information that could be considered context information.

5.2. Classification of events, failures, and attacks

It is hard to differentiate between various anomalies in industrial control systems because their effects are similar. However, this task might be possible with the benefits of IIoT, as it allows collecting a large amount of data from the environment through sensors Wang et al. (2021a). Differentiating anomalies is necessary to select an appropriate action in component reconfiguration, estimate a level of propagation in the system, and avoid bad reactions that can worsen the system state. Due to strict real-time requirements in industrial systems, it is imperative to reduce response times to attend to an anomaly in critical infrastructure. That is why fast and accurate detection and classification of anomalies are important Moradbeikie et al. (2020).

Several authors have contributed to detecting events, failures, or attacks in IIoT systems. Some reports detect general anomalies, while others focus on a particular type of anomaly. We have found that most of the works analyzed in this review focus on malicious attack detection, a smaller percentage detects faults in IIoT systems, and an even smaller portion detects events occurring in the application context, as shown in Fig. 2. In the scope of our review, we could not find any work that classifies events, failures, and attacks with the same algorithm.

Analyzing and differentiating the anomaly source is crucial since all these anomalies coexist in the industrial system. The above allows the system operator to choose appropriate recovery actions to counteract the abnormal behavior. Traditionally, fault diagnosis is based on the operator's experience. Nevertheless, systems are becoming increasingly complex and interconnected. Hence, it is necessary to add automatic diagnostic functions to avoid relying on the availability of trained operators Tertytchny et al. (2020).

Some reports perform a dual task. On the one hand, they classify the data generated by the IoT system as normal or abnormal. On the other hand, they classify the specific type of attack. Authors in Abu Al-Haija and Zein-Sabatto (2020) propose an approach to detect and

Table 5
Anomaly detection proposals using deep learning methods (E stands for Events, F stands for Failures, and A stands for Attacks).

Reference	Anomaly detection strategy	Anomaly	Classify (E-F-A)	Context Aware	Detection Layer	Execute Layer
Sankaran and Kim (2023)	Multi-cascaded CNN classification	Attacks	✓*	✗	Network	-
Çavdar et al. (2023)	1D convolution neural networks and the Dempster–Shafer	Failures	✓*	✗	Device	-
Halder and Newe (2023)	Federated learning with GRU	Attacks	✗	✗	Network	Local server
Kumar et al. (2023)	An adaptive transformer model for anomaly detection	Attacks	✗	✗	Network	-
Kim et al. (2023)	Stacked Transformer representations and 1D Convolutional network	Failures	✗	✗	Application	-
Ba et al. (2022b)	Automated Configuration of Heterogeneous Graph Neural Networks	All	✗	✗	Device	-
Ba et al. (2022a)	Transformer-based Graph Convolutional Neural Networks	All	✗	✗	Network	-
Truong et al. (2022)	Light-weight federated learning-based anomaly detection	All	✗	✗	Device	Edge
Hu et al. (2022)	Transfer Learning based Trajectory Anomaly Detection	All	✗	✗	Device	Edge
Pan et al. (2022)	Dual masked self-attention mechanism	All	✗	✗	Device	-
Feng et al. (2022)	A full graph autoencoder	All	✗	✗	Device	-
Nizam et al. (2022)	Convolutional neural network and a two-stage LSTM based Autoencoder	All	✗	✗	Device	-
Mukherjee (2022)	Deep learning models to determine the exact intrusion points in real-time	Attacks	✗	✗	Device	-
Nedeljkovic and Jakovljevic (2022)	Method for calculating the hyper parameters of CNN to detect cyber-attacks	Attacks	✗	✗	Network	Device
Weinger et al. (2022)	Data augmentation in federated learning for anomaly detection	All	✗	✗	Device	Edge
Friha et al. (2022)	Federated learning-based decentralized intrusion detection system	Attacks	✗	✗	Network	Edge
Liu et al. (2022)	DDoS detection with information entropy analysis	Attacks	✗	✗	Network	-
Yang et al. (2022a)	One-class broad learning system	Attacks	✗	✗	Network	-
Chen et al. (2021)	Learning Graph Structures With Transformer	Attacks	✗	✗	Device	-
Wangwang et al. (2021)	Network Traffic Oriented Malware Detection	Attacks	✗	✗	Network	-
Kozik et al. (2021)	A hybrid time window embedding with transformer-based traffic data classification	Attacks	✗	✗	Network	-
Wang et al. (2021a)	Hierarchical Federated Learning	Attacks	✗	✗	Device	-
Wang et al. (2021b)	Unknown attack Identification using spatial-temporal features	Attacks	✗	✗	Network	-
Huong et al. (2021)	VAE-LSTM model on edge devices	Attacks	✗	✗	Device	Edge
Kong et al. (2021)	Generative adversarial networks	All	✗	✗	Network	-
Wang et al. (2021a)	Federated deep reinforcement Learning	Attacks	✗	✗	Network	-
Khan et al. (2021)	Temporal and spatial features for the classification and explanation attacks	Attacks	✗	✗	Network	-
Ketonen and Blech (2021)	Probabilistic Deep Learning	All	✗	✗	Device	-
Liu et al. (2020a)	Attention Mechanism-Based CNN Unit and LSTM Unit	All	✗	✗	Device	Edge
Savic et al. (2021)	Autoencoder in edge device	All	✗	✗	Device	Edge
Seo et al. (2021)	Acoustic-Based Anomaly Detection	Attacks	✗	✗	Device	Edge
Dzaferagic et al. (2021)	Generative Adversarial Networks to generate missing sensor measurements	Failures	✗	✗	Device	-
Wu et al. (2021)	Graph Neural Networks	All	✗	✗	Device	Edge & Cloud
Zhou et al. (2020)	LSTM to mitigate dimensional reduction in unbalanced data	All	✗	✗	Network	-
Li et al. (2020b)	multi-CNN fusion	Attacks	✗	✗	Network	-
Park et al. (2020)	Setting boundaries based on cosine similarity in network packets	All	✗	✗	Network	-
Wu et al. (2019)	LSTM with Bayesian and Gaussian Processing	All	✗	✗	Device	-
Li et al. (2020a)	Bidirectional long and short-term memory (B-LSTM)	Attacks	✗	✗	Network	Local server
Liu et al. (2020a)	On-device collaborative deep anomaly detection	Failures	✗	✗	Device	Edge
Demertzis et al. (2020)	Blockchained deep learning smart contracts	All	✗	✓	Application	Cloud
De Vita et al. (2020b)	DeepAutoencoder and PCA blocks	Failures	✗	✗	Device	Edge & Cloud
Liu et al. (2020b)	Federated Learning to collaboratively train a Deep Anomaly Detection	All	✗	✗	Device	Edge
Wang et al. (2020b)	Recurrent neural networks	Failures	✗	✗	Device	Edge
Ferrari et al. (2019)	Compare LSTM on edge and cloud	Failures	✗	✗	Device	Edge & Cloud
Liu et al. (2019)	Gated Recurrent Unit (GRU) and Support Vector Domain Description	Attacks	✗	✗	Network	-
Bernieri et al. (2019b)	Variational Autoencoders(VAE)	Attacks	✗	✗	Network	-
Al-Hawawreh and Sitnikova (2019)	Variational Auto-Encoder learns the latent structure of system activities	Attacks	✗	✗	Network	-
Krundyshev and Kalinin (2019)	Determining the normal (legitimate) activity of nodes	Attacks	✗	✗	Network	-
Bae et al. (2018)	Autoencoder with invasion scoring	Attacks	✗	✗	Network	-
Al-Hawawreh et al. (2019)	Sparse and denoising autoencoder	All	✗	✗	Network	Local server
Kim et al. (2018)	Squeezed Convolutional Variational AutoEncoder	All	✗	✗	Device	Edge
Saurav et al. (2018)	Recurrent Neural Networks Recurrent Units (GRU)	All	✗	✗	Network	-
Muna et al. (2018)	Deep Auto-Encoder (DAE)	Attacks	✗	✗	Network	Cloud
Schneider and Böttinger (2018)	Stacked denoising autoencoder	Attacks	✗	✗	Network	Edge
Tandiya et al. (2018)	Frequency-domain data are transformed in 2D image	Attacks	✗	✗	Network	Edge

Methods marked with * classify anomalies but without identifying the three kinds of anomalies defined in this review.

classify cyber-attacks in IoT communication networks NSL-KDD dataset, using convolutional neural networks running in a Compute Unified Device Architecture (CUDA) based on Nvidia GPUs (Graphical Processing Units). In Abu Al-Haija and Al-Dala'ien (2022) authors classify botnet attacks in N-BaIoT2021 dataset, using four machine-learning-based decision tree models: AdaBoosted, RUSBoosted, bagged, and their ensemble learning model. Likewise, Abu Al-Haija et al. (2022) use AdaBoost machine learning algorithms combined with Decision Trees to classify some attacks in an IIoT dataset, such as DoS, DDoS, MitM, backdoor, and injection. Whereas, Albulayhi et al. (2022) analyze how feature selection increases detection accuracy and speed training phase. They test their proposed classifying between Mirai, DoS, Scan, MAS (MitM-ARP Spoofing) attacks, and normal operation.

Other proposals differentiate between physical failures and cyber-attacks in Cyber-Physical Systems (CPS). The authors in Tertytchny et al. (2020) study the problem of distinguishing between component failures and attacks on the communication network in a power-aware intelligent home system, analyzing the correlation between failures and attacks and providing a framework. Authors consider that a normal state occurs when all variables are within the expected limits (no failures) and the nodes are connected to a central node (no attacks). However, this research shows that if the effects of failures and attacks are similar, they cannot be differentiated for their framework.

Authors in Moradbeikie et al. (2020) propose to classify sensor anomalies into four categories such as stealth attacks, random attacks, temporary failures, and permanent failures, and then automatically reconfigure the system to react to an anomaly. The proposal has three components such as risk detection (comparing the received values with a threshold outside of which it is classified as abnormal), risk analysis (calculates the probability for each type of risk and its level of damage according to a propagation of the risk, taking into account that the measured variables follow physical laws) and system reconfiguration (if a group of damage is above a tolerance threshold, the system reacts). The solution requires a deep knowledge of the system to determine the different states it takes, and the time it remains in each one Moradbeikie et al. (2020). Notice that even though this proposal defines four categories, it does not classify among events. Another work is presented in Miciolino et al. (2017), where authors propose a system to detect physical failures and cyber-attacks in critical infrastructure; for this, they use a testbed that simulates a water plant with highly nonlinear variables and very slow dynamics. With the data collected by a SCADA system, the authors investigate how the monitoring modules react to different physical and cyber problems while also analyzing cross effects. First, normal system behavior data and statistical trends of the water level in each tank are collected. Incoming data is compared with expected data; the information is considered abnormal if the difference exceeds a threshold value. To differentiate between failure and attack, the researchers assume that physical failures influence the variable related to the component involved. In contrast, attacks can be reflected in different system behaviors.

6. Open challenges

Although detecting anomalies in IIoT are a widely discussed topic, implementing these algorithms in IIoT devices are still an open issue. Designing a real-time online anomaly detection system on an end- or edge device is still challenging because of the limitations that impose the constrained resources of these platforms, which restrain the amount of data available and the algorithm's complexity. Real-time cloud solutions present other challenges. For instance, the exhaustive use of bandwidth, which is not always available on IoT devices, and the high latency of the communication link, affect real-time constraints. The main questions are: how to implement a real-time anomaly detector using a constrained IIoT device? What are the most appropriate ML or DL methods to deploy at the edge of the cloud?

Another exciting result of this review is that automatically classifying anomalies as events, failures, or attacks remains an open research subject. This classification is crucial to address the anomaly to the correct department in the industry, enhancing the response times and the efficiency of the process. The production department handles events, maintenance staff solves failures, and the IT department counters attacks. Some interesting questions around this topic are: What makes failures, events, or malicious attacks statistically different? What is the signature of each of these types of anomaly? How to do spatial and temporal correlation help to differentiate the origin of an anomaly? How much labeled abnormal data suffices to train a classification model? Which device could execute the classification algorithm?

Context awareness can help detect spatial, sequential, and temporal attributes between devices and better characterize the current state of devices. Although some authors have stated that context information helps implement anomaly detection and classification, there are few systems using it already. We found that automatic anomaly classification in IIoT is an open research topic, and additional information from the application context is rarely used to facilitate anomaly detection. Finding data sets incorporating variables describing the application context is also challenging. Some essential questions are: how does context information help to detect and classify IIoT anomalies? Does the improvement in anomaly classifier performance justify the cost of recording and processing additional context variables?

Finally, new labeled data sets are needed to advance in implementing statistical and machine-learning techniques for detecting and classifying various anomalies. It is necessary to have datasets, including network data and data from physical variables collected by sensors, adequately labeled as normal, event, fault, or attack. Here are some questions that need to be answered: how complex an IIoT testbed shall be to collect a dataset for classifying anomalies? Is it possible to generate these datasets through simulated IIoT environments? Can a desktop or online application create simulations to obtain these datasets?

7. Conclusion

This paper reviewed the state-of-the-art for anomaly detection and classification systems in the Industrial IoT. We studied 99 articles in the literature from 2018 to 2023. We defined criteria for analyzing the papers, including the method's ability to detect or classify anomalies and the layer in which the detection/classification is performed and executed.

According to our results, automatic diagnosis of the anomaly origin is still an open research topic. Several authors use statistical and machine-learning techniques to detect anomalies. However, we found a few reports that classify the source of an anomaly as a fault or an attack. In addition, none of the papers consider event classification; they need to address its definition. We also identified the scarce use of data that can be regarded as context information to help detect spatial, sequential, and temporal attributes among IIoT variables and improve anomaly detection.

As a prospectus for future research, our aim is to delve deeper into particular facets of anomaly classification, primarily concerning the implementation of a real-time anomaly detector using a limited IIoT device. In addition, we aspire to identify the factors that differentiate failures, events, and attacks statistically, the role of contextual information in identifying and categorizing IIoT anomalies, and the development of an IIoT testbed to collect datasets for the purpose of classifying anomalies.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

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.

Data availability

Data will be made available on request.

References

Abu Al-Haija, Q., Al Badawi, A., & Bojja, G. R. (2022). Boost-defence for resilient iot networks: A head-to-toe approach. *Expert Systems*, *39*(10), Article e12934. https://doi.org/10.1111/exsy.12934.

Abu Al-Haija, Q., & Al-Dala'ien, M. (2022). Elba-iot: An ensemble learning model for botnet attack detection in iot networks. *Journal of Sensor and Actuator Networks*, *11*(1), 18. https://doi.org/10.3390/jsan11010018.

Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics*, *9*(12), 2152. https://doi.org/10.3390/electronics9122152.

Ahakonye, L. A. C., Nwakanma, C. I., Lee, J.-M., & Kim, D.-S. (2023a). Scada intrusion detection scheme exploiting the fusion of modified decision tree and chi-square feature selection. *Internet of Things*, *21*, Article 100676. https://doi.org/10.1016/j.iot.2022.100676.

Ahakonye, L. A. C., Nwakanma, C. I., Lee, J. M., & Kim, D.-S. (2023b). Agnostic ch-dt technique for scada network high-dimensional data-aware intrusion detection system. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2023.3237797.

Al-Hawawreh, M., & Sitnikova, E. (2019). Industrial Internet of things based ransomware detection using stacked variational neural network. In *Proceedings of the 3rd international conference on big data and Internet of things* (pp. 126–130).

Al-Hawawreh, M., Sitnikova, E., & den Hartog, F. (2019). An efficient intrusion detection model for edge system in brownfield industrial Internet of things. In *Proceedings of the 3rd international conference on big data and Internet of things* (pp. 83–87).

Albulayhi, K., Abu Al-Haija, Q., Alsuhibany, S. A., Jillepalli, A. A., Ashrafuzzaman, M., & Sheldon, F. T. (2022). Iot intrusion detection using machine learning with a novel high performing feature selection method. *Applied Sciences*, *12*(10), 5015. https://doi.org/10.3390/app12105015.

Alexopoulos, K., Sipsas, K., Xanthakis, E., Makris, S., & Mourtzis, D. (2018). An industrial Internet of things based platform for context-aware information services in manufacturing. *International Journal of Computer Integrated Manufacturing*, *31*(11), 1111–1123. https://doi.org/10.1080/0951192X.2018.1500716.

Alruwaili, F. F. (2021). Intrusion detection and prevention in industrial iot: A technological survey. In *2021 international conference on electrical, computer, communications and mechatronics engineering (ICECCME)* (pp. 1–5). IEEE.

Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., & Zahariadis, T. (2020). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. *Sensors*, *20*(1), 109. https://doi.org/10.3390/s20010109.

Anton, S. D., Fraunholz, D., Schotten, H. D., & Teuber, S. (2017). A question of context: Enhancing intrusion detection by providing context information. In *2017 Internet of things business models, users, and networks* (pp. 1–8). IEEE.

Anton, S. D. D., Lohfink, A. P., Garth, C., & Schotten, H. D. (2019). Security in process: Detecting attacks in industrial process data. In *Proceedings of the third central European cybersecurity conference* (pp. 1–6).

Aoudi, W., & Almgren, M. (2020). A scalable specification-agnostic multi-sensor anomaly detection system for iiot environments. *International Journal of Critical Infrastructure Protection*, *30*, 1–8. https://doi.org/10.1016/j.ijcip.2020.100377.

Aranda, J. A. S., dos Santos Costa, R., de Vargas, V. W., da Silva Pereira, P. R., Barbosa, J. L. V., & Vianna, M. P. (2022). Context-aware edge computing and Internet of things in smart grids: A systematic mapping study. *Computers & Electrical Engineering*, *99*, Article 107826. https://doi.org/10.1016/j.compeleceng.2022.107826.

Aruquipa, G., & Diaz, F. (2022). An iot architecture based on the control of bio inspired manufacturing system for the detection of anomalies with vibration sensors. *Procedia Computer Science*, *200*, 438–450. https://doi.org/10.1016/j.procs.2022.01.242.

Ba, A., Lorenzi, F., & Ploennigs, J. (2022a). Monitoring of iot systems at the edges with transformer-based graph convolutional neural networks. In *2022 IEEE international conference on edge computing and communications* (pp. 41–49). EDGE: IEEE.

Ba, A., Lynch, K., Ploennigs, J., Schaper, B., Lohse, C., & Lorenzi, F. (2022b). Automated configuration of heterogeneous graph neural networks with a semantic math parser for iot systems. *IEEE Internet of Things Journal*, *10*(2), 1042–1052. https://doi.org/10.1109/JIOT.2022.3204889.

Bae, G., Jang, S., Kim, M., & Joe, I. (2018). Autoencoder-based on anomaly detection with intrusion scoring for smart factory environments. In *International conference on parallel and distributed computing: Applications and technologies* (pp. 414–423). Springer.

Bernieri, G., Conti, M., & Pozzan, G. (2019a). Amon: An automaton monitor for industrial cyber-physical security. In *Proceedings of the 14th international conference on availability, reliability and security* (pp. 1–10).

Bernieri, G., Conti, M., & Turrin Kingfisher, F. (2019b). An industrial security framework based on variational autoencoders. In *Proceedings of the 1st workshop on machine learning on edge in sensor systems* (pp. 7–12).

Bernieri, G., & Pascucci, F. (2019). Improving security in industrial Internet of things: A distributed intrusion detection methodology. In *Security and privacy trends in the industrial Internet of things* (pp. 161–179). Springer.

Bodo, R., Bertocco, M., & Bianchi, A. (2020). Feature ranking under industrial constraints in continuous monitoring applications based on machine learning techniques. In *2020 IEEE international instrumentation and measurement technology conference (I2MTC)* (pp. 1–6). IEEE.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of things: A survey. *Future Generations Computer Systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of things (iiot): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015.

Cai, J., Wang, Q., Luo, J., Liu, Y., & Liao, L. (2021). Capbad: Content-agnostic, payload-based anomaly detector for industrial control protocols. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3138534.

Çavdar, T., Ebrahimpour, N., Kakız, M. T., & Günay, F. B. (2023). Decision-making for the anomalies in iiots based on 1d convolutional neural networks and Dempster–Shafer theory (ds-1dcnn). *Journal of Supercomputing*, *79*(2), 1683–1704. https://doi.org/10.1007/s11227-022-04739-2.

Chen, Z., Chen, D., Zhang, X., Yuan, Z., & Cheng, X. (2021). Learning graph structures with transformer for multivariate time-series anomaly detection in iot. *IEEE Internet of Things Journal*, *9*(12), 9179–9189. https://doi.org/10.1109/JIOT.2021.3100509.

Cui, J-f., Xia, H., Zhang, R., Hu, B-x., & Cheng, X-g. (2021). Optimization scheme for intrusion detection scheme gbdt in edge computing center. *Computer Communications*, *168*, 136–145. https://doi.org/10.1016/j.comcom.2020.12.007.

Dang, T.-B., Le, D.-T., Kim, M., & Choo, H. (2021). Neighboring information exploitation for anomaly detection in intelligent iot. In *International conference on future data and security engineering* (pp. 260–271). Springer.

De, S., Bermudez-Edo, M., Xu, H., & Cai, Z. (2022). Deep generative models in the industrial Internet of things: A survey. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2022.3155656.

De Vita, F., Bruneo, D., & Das, S. K. (2020a). On the use of a full stack hardware/software infrastructure for sensor data fusion and fault prediction in industry 4.0. *Pattern Recognition Letters*, *138*, 30–37. https://doi.org/10.1016/j.patrec.2020.06.028.

De Vita, F., Bruneo, D., & Das, S. K. (2020b). A novel data collection framework for telemetry and anomaly detection in industrial iot systems. In *2020 IEEE/ACM fifth international conference on Internet-of-things design and implementation (IoTDI)* (pp. 245–251). IEEE.

De Vita, F., Bruneo, D., & Das, S. K. (2021). A semi-supervised Bayesian anomaly detection technique for diagnosing faults in industrial iot systems. In *2021 IEEE international conference on smart computing (SMARTCOMP)* (pp. 31–38). IEEE.

DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of ai-based anomaly detection in iot and sensor networks. *Sensors*, *23*(3), 1352. https://doi.org/10.3390/s23031352.

Demertzis, K., Iliadis, L., Tziritas, N., & Kikiras, P. (2020). Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Computing & Applications*, *32*(23), 17361–17378. https://doi.org/10.1007/s00521-020-05189-8.

Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M. (2023). An improved anomaly detection model for iot security using decision tree and gradient boosting. *Journal of Supercomputing*, *79*(3), 3392–3411. https://doi.org/10.1007/s11227-022-04783-y.

Dzaferagic, M., Marchetti, N., & Macaluso, I. (2021). Fault detection and classification in industrial iot in case of missing sensor data, https://doi.org/10.1109/JIOT.2021.3116785.

Ehsani-Besheli, F., & Zarandi, H. R. (2017). Context-aware anomaly detection in embedded systems. In *Advances in dependability engineering of complex systems* (pp. 151–165). Springer.

Elnour, M., Meskin, N., Khan, K., & Jain, R. (2021). Application of data-driven attack detection framework for secure operation in smart buildings. *Sustainable Cities and Society*, *69*, Article 102816. https://doi.org/10.1016/j.scs.2021.102816.

Enăchescu, C., Sándor, H., & Genge, B. (2019). A multi-model-based approach to detect cyber stealth attacks in industrial Internet of things. In *2019 international conference on software, telecommunications and computer networks (SoftCOM)* (pp. 1–6). IEEE.

Fahim, M., & Sillitti, A. (2019). Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. *IEEE Access*, *7*, 81664–81681. https://doi.org/10.1109/ACCESS.2019.2921912.

Faisal, M. A., Cardenas, A. A., & Wool, A. (2019). Profiling communications in industrial ip networks: Model complexity and anomaly detection. In *Security and privacy trends in the industrial Internet of things* (pp. 139–160). Springer.

Feng, Y., Chen, J., Liu, Z., Lv, H., & Wang, J. (2022). Full graph autoencoder for one-class group anomaly detection of iiot system. *IEEE Internet of Things Journal*, *9*(21), 21886–21898. https://doi.org/10.1109/JIOT.2022.3181737.

Ferrari, P., Rinaldi, S., Sisinni, E., Colombo, F., Ghelfi, F., Maffei, D., & Malara, M. (2019). Performance evaluation of full-cloud and edge-cloud architectures for industrial iot anomaly detection based on deep learning. In *2019 II workshop on metrology for industry 4.0 and IoT (MetroInd4. 0&IoT)* (pp. 420–425). IEEE.

Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., Choo, K.-K. R., & Nafaa, M. (2022). Felids: Federated learning-based intrusion detection system for agricultural Internet of

things. *Journal of Parallel and Distributed Computing*. https://doi.org/10.1016/j.jpdc.2022.03.003.

Gai, F., Zhang, J., Zhu, P., & Jiang, X. (2017). Multidimensional trust-based anomaly detection system in Internet of things. In *International conference on wireless algorithms, systems, and applications* (pp. 302–313). Springer.

Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A. (2020). A multi-stage anomaly detection scheme for augmenting the security in iot-enabled applications. *Future Generations Computer Systems*, *104*, 105–118. https://doi.org/10.1016/j.future.2019.09.038.

Garitano, I., Iturbe, M., Ezpeleta, E., & Zurutuza, U. (2019). Who's there? Evaluating data source integrity and veracity in iiot using multivariate statistical process control. In *Security and privacy trends in the industrial Internet of things* (pp. 181–198). Springer.

Garmaroodi, M. S. S., Farivar, F., Haghighi, M. S., Shoorehdeli, M. A., & Jolfaei, A. (2020). Detection of anomalies in industrial iot systems by data mining: Study of christ osmotron water purification system. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.3034311.

Genge, B., Haller, P., & Enăchescu, C. (2019). Anomaly detection in aging industrial Internet of things. *IEEE Access*, *7*, 74217–74230. https://doi.org/10.1109/ACCESS.2019.2920699.

Ghaeini, H. R., Antonioli, D., Brasser, F., Sadeghi, A.-R., & Tippenhauer, N. O. (2018). State-aware anomaly detection for industrial control systems. In *Proceedings of the 33rd annual ACM symposium on applied computing* (pp. 1620–1628).

Ghosh, N., Maity, K., Paul, R., & Maity, S. (2019). Outlier detection in sensor data using machine learning techniques for iot framework and wireless sensor networks: A brief study. In *2019 international conference on applied machine learning (ICAML)* (pp. 187–190). IEEE.

Gorbenko, A., & Popov, V. (2020). Abnormal behavioral pattern detection in closed-loop robotic systems for zero-day deceptive threats. In *2020 international conference on industrial engineering, applications and manufacturing (ICIEAM)* (pp. 1–6). IEEE.

Halder, S., & Newe, T. (2023). Radio fingerprinting for anomaly detection using federated learning in lora-enabled industrial Internet of things. In *Future generation computer systems*.

Hansch, G., Schneider, P., & Brost, G. S. (2019). Deriving impact-driven security requirements and monitoring measures for industrial iot. In *Proceedings of the 5th on cyber-physical system security workshop* (pp. 37–45).

Hashmat, F., Abbas, S. G., Hina, S., Shah, G. A., Bakhshi, T., & Abbas, W. (2022). An automated context-aware iot vulnerability assessment rule-set generator. *Computer Communications*, *186*, 133–152. https://doi.org/10.1016/j.comcom.2022.01.022.

Hayes, M. A., & Capretz, M. A. (2014). Contextual anomaly detection in big sensor data. In *2014 IEEE international congress on big data* (pp. 64–71). IEEE.

He, J., Kong, L., Frondelius, T., Silvén, O., & Juntti, M. (2020). Decision triggered data transmission and collection in industrial Internet of things. In *2020 IEEE wireless communications and networking conference (WCNC)* (pp. 1–5). IEEE.

Hu, J., Kaur, K., Lin, H., Wang, X., Hassan, M. M., Razzak, I., & Hammoudeh, M. (2022). Intelligent anomaly detection of trajectories for iot empowered maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3162491.

Huong, T. T., Bac, T. P., Long, D. M., Luong, T. D., Dan, N. M., Thang, B. D., Tran, K. P., et al. (2021). Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach. *Computers in Industry*, *132*, Article 103509. https://doi.org/10.1016/j.compind.2021.103509.

Karkouch, A., Mousannif, H., Al Moatassime, H., & Noel, T. (2016). Data quality in Internet of things: A state-of-the-art survey. *Journal of Network and Computer Applications*, *73*, 57–81. https://doi.org/10.1016/j.jnca.2016.08.002.

Ketonen, V., & Blech, J. O. (2021). Anomaly detection for injection molding using probabilistic deep learning. In *2021 4th IEEE international conference on industrial cyber-physical systems (ICPS)* (pp. 70–77). IEEE.

Khan, I. A., Moustafa, N., Pi, D., Sallam, K. M., Zomaya, A. Y., & Li, B. (2021). A new explainable deep learning framework for cyber threat discovery in industrial iot networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3130156.

Kim, D., Yang, H., Chung, M., Cho, S., Kim, H., Kim, M., Kim, K., & Kim, E. (2018). Squeezed convolutional variational autoencoder for unsupervised anomaly detection in edge device industrial Internet of things. In *2018 international conference on information and computer technologies (icict)* (pp. 67–71). IEEE.

Kim, J., Kang, H., & Kang, P. (2023). Time-series anomaly detection with stacked transformer representations and 1d convolutional network. *Engineering Applications of Artificial Intelligence*, *120*, Article 105964. https://doi.org/10.1016/j.engappai.2023.105964.

Kong, F., Li, J., Jiang, B., Wang, H., & Song, H. (2021). Integrated generative model for industrial anomaly detection via bi-directional lstm and attention mechanism. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2021.3078192.

Kozik, R., Pawlicki, M., & Choraś, M. (2021). A new method of hybrid time window embedding with transformer-based traffic data classification in iot-networked environment. *Pattern Analysis & Applications*, *24*(4), 1441–1449. https://doi.org/10.1007/s10044-021-00980-2.

Krundyshev, V., & Kalinin, M. (2019). Hybrid neural network framework for detection of cyber attacks at smart infrastructures. In *Proceedings of the 12th international conference on security of information and networks* (pp. 1–7).

Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. (2022). Machine learning-based early detection of iot botnets using network-edge traffic. *Computers & Security*, Article 102693. https://doi.org/10.1016/j.cose.2022.102693.

Kumar, A. S., Raja, S., Pritha, N., Raviraj, H., Lincy, R. B., & Rubia, J. J. (2023). An adaptive transformer model for anomaly detection in wireless sensor networks in real-time. *Measurement: Sensors*, *25*, Article 100625. https://doi.org/10.1016/j.measen.2022.100625.

Langone, R., Cuzzocrea, A., & Skantzos, N. (2020). Interpretable anomaly prediction: Predicting anomalous behavior in industry 4.0 settings via regularized logistic regression tools. *Data & Knowledge Engineering*, *130*, Article 101850. https://doi.org/10.1016/j.datak.2020.101850.

Li, X., Xu, M., Vijayakumar, P., Kumar, N., & Liu, X. (2020a). Detection of low-frequency and multi-stage attacks in industrial Internet of things. *IEEE Transactions on Vehicular Technology*, *69*(8), 8820–8831. https://doi.org/10.1109/TVT.2020.2995133.

Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., & Cui, L. (2020b). Robust detection for network intrusion of industrial iot based on multi-cnn fusion. *Measurement*, *154*, Article 107450. https://doi.org/10.1016/j.measurement.2019.107450.

Li, Z., Ding, X., & Wang, H. (2020c). An effective constraint-based anomaly detection approach on multivariate time series. In *Asia-Pacific web (APWeb) and web-age information management (WAIM) joint international conference on web and big data* (pp. 61–69). Springer.

Liu, S., Chen, X., Peng, X., & Xiao, R. (2019). Network log anomaly detection based on gru and svdd. In *2019 IEEE intl conf on parallel & distributed processing with applications, big data & cloud computing, sustainable computing & communications, social computing & networking (ISPA/BDCloud/SocialCom/SustainCom)* (pp. 1244–1249). IEEE.

Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J., & Hossain, M. S. (2020a). Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, *8*(8), 6348–6358. https://doi.org/10.1109/JIOT.2020.3011726.

Liu, Y., Kumar, N., Xiong, Z., Lim, W. Y. B., Kang, J., & Niyato, D. (2020b). Communication-efficient federated learning for anomaly detection in industrial Internet of things. In *GLOBECOM 2020-2020 IEEE global communications conference* (pp. 1–6). IEEE.

Liu, Y., Zhi, T., Shen, M., Wang, L., Li, Y., & Wan, M. (2022). Software-defined ddos detection with information entropy analysis and optimized deep learning. *Future Generations Computer Systems*, *129*, 99–114. https://doi.org/10.1016/j.future.2021.11.009.

Madhawa, S., Balakrishnan, P., & Arumugam, U. (2018). Employing invariants for anomaly detection in software defined networking based industrial Internet of things. *Journal of Intelligent & Fuzzy Systems*, *35*(2), 1267–1279. https://doi.org/10.3233/JIFS-169670.

Miciolino, E. E., Setola, R., Bernieri, G., Panzieri, S., Pascucci, F., & Polycarpou, M. M. (2017). Fault diagnosis and network anomaly detection in water infrastructures. *IEEE Design & Test*, *34*(4), 44–51. https://doi.org/10.1109/MDAT.2017.2682223.

Mohamudally, N., & Peermamode-Mohaboob, M. (2018). Building an anomaly detection engine (ade) for iot smart applications. *Procedia Computer Science*, *134*, 10–17. https://doi.org/10.1016/j.procs.2018.07.138.

Moradbeikie, A., Jamshidi, K., Bohlooli, A., Garcia, J., & Masip-Bruin, X. (2020). An iiot based ics to improve safety through fast and accurate hazard detection and differentiation. *IEEE Access*, *8*, 206942–206957. https://doi.org/10.1109/ACCESS.2020.3037093.

Mukherjee, D. (2022). A novel strategy for locational detection of false data injection attack. *Sustainable Energy, Grids and Networks*, Article 100702. https://doi.org/10.1016/j.segan.2022.100702.

Muna, A.-H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial Internet of things based on deep learning models. *Journal of Information Security and Applications*, *41*, 1–11. https://doi.org/10.1016/j.jisa.2018.05.002.

Nedeljkovic, D., & Jakovljevic, Z. (2022). Cnn based method for the development of cyber-attacks detection algorithms in industrial control systems. *Computers & Security*, *114*, Article 102585. https://doi.org/10.1016/j.cose.2021.102585.

Nizam, H., Zafar, S., Lv, Z., Wang, F., & Hu, X. (2022). Real-time deep anomaly detection framework for multivariate time-series data in industrial iot. *IEEE Sensors Journal*, *22*(23), 22836–22849. https://doi.org/10.1109/JSEN.2022.3211874.

Ouyang, Z., Sun, X., Chen, J., Yue, D., & Zhang, T. (2018). Multi-view stacking ensemble for power consumption anomaly detection in the context of industrial Internet of things. *IEEE Access*, *6*, 9623–9631. https://doi.org/10.1109/ACCESS.2018.2805908.

Pan, J., Ji, W., Zhong, B., Wang, P., Wang, X., & Chen Duma, J. (2022). Dual mask for multivariate time series anomaly detection. *IEEE Sensors Journal*. https://doi.org/10.1109/JSEN.2022.3225338.

Park, S. H., Park, H. J., & Choi, Y.-J. (2020). Rnn-based prediction for network intrusion detection. In *2020 international conference on artificial intelligence in information and communication (ICAIIC)* (pp. 572–574). IEEE.

Peng, Y., Tan, A., Wu, J., & Bi, Y. (2019). Hierarchical edge computing: A novel multi-source multi-dimensional data anomaly detection scheme for industrial Internet of things. *IEEE Access*, *7*, 111257–111270. https://doi.org/10.1109/ACCESS.2019.2930627.

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, *64*, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007.

Raposo, D., Rodrigues, A., Sinche, S., Silva, J. S., & Boavida, F. (2018). Securing wirelesshart: Monitoring, exploring and detecting new vulnerabilities. In *2018 IEEE 17th international symposium on network computing and applications (NCA)* (pp. 1–9). IEEE.

Raposo, D., Rodrigues, A., Sinche, S., Silva, J. S., & Boavida, F. (2019). Security and fault detection in in-node components of iiot constrained devices. In *2019 IEEE 44th conference on local computer networks (LCN)* (pp. 282–290). IEEE.

Razzak, I., Zafar, K., Imran, M., & Xu, G. (2020). Randomized nonlinear one-class support vector machines with bounded loss function to detect of outliers for large scale iot data. *Future Generations Computer Systems*, *112*, 715–723. https://doi.org/10.1016/j.future.2020.05.045.

Rey, V., Sánchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in iot devices. *Computer Networks*, Article 108693. https://doi.org/10.1016/j.comnet.2021.108693.

Rousopoulou, V., Vafeiadis, T., Nizamis, A., Iakovidis, I., Samaras, L., Kirtsoglou, A., Georgiadis, K., Ioannidis, D., & Tzovaras, D. (2022). Cognitive analytics platform with ai solutions for anomaly detection. *Computers in Industry*, *134*, Article 103555. https://doi.org/10.1016/j.compind.2021.103555.

Sankaran, K. S., & Kim, B.-H. (2023). Deep learning based energy efficient optimal rmc-cnn model for secured data transmission and anomaly detection in industrial iot. *Sustainable Energy Technologies and Assessments*, *56*, Article 102983. https://doi.org/10.1016/j.seta.2022.102983.

Saurav, S., Malhotra, P., TV, V., Gugulothu, N., Vig, L., Agarwal, P., & Shroff, G. (2018). 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* (pp. 78–87).

Savic, M., Lukic, M., Danilovic, D., Bodroski, Z., Bajović, D., Mezei, I., Vukobratovic, D., Skrbic, S., & Jakovetić, D. (2021). Deep learning anomaly detection for cellular iot with applications in smart logistics. *IEEE Access*, *9*, 59406–59419. https://doi.org/10.1109/ACCESS.2021.3072916.

Schneider, P., & Böttinger, K. (2018). High-performance unsupervised anomaly detection for cyber-physical system networks. In *Proceedings of the 2018 workshop on cyber-physical systems security and privacy* (pp. 1–12).

Seo, C.-B., Lee, G., Lee, Y., & Seo, S.-H. (2021). Echo-guard: Acoustic-based anomaly detection system for smart manufacturing environments. In *International conference on information security applications* (pp. 64–75). Springer.

Shi, Y., Li, F., Song, W., Li, X.-Y., & Ye, J. (2019). Energy audition based cyber-physical attack detection system in iot. In *Proceedings of the ACM Turing celebration conference-China* (pp. 1–5).

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491.

Su, J., He, S., & Wu, Y. (2022). Features selection and prediction for iot attacks. *High-Confidence Computing*, *2*(2), Article 100047. https://doi.org/10.1016/j.hcc.2021.100047.

Sun, P., Yuepeng, E., Li, T., Wu, Y., Ge, J., You, J., & Wu, B. (2020). Context-aware learning for anomaly detection with imbalanced log data. In *2020 IEEE 22nd international conference on high performance computing and communications, IEEE 18th international conference on smart city, IEEE 6th international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 449–456). IEEE.

Tandiya, N., Jauhar, A., Marojevic, V., & Reed, J. H. (2018). Deep predictive coding neural network for rf anomaly detection in wireless networks. In *2018 IEEE international conference on communications workshops (ICC workshops)* (pp. 1–6). IEEE.

Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in iot-based cyber physical systems using machine learning. *Microprocessors and Microsystems*, *77*, Article 103121. https://doi.org/10.1016/j.micpro.2020.103121.

Truong, H. T., Ta, B. P., Le, Q. A., Nguyen, D. M., Le, C. T., Nguyen, H. X., Do, H. T., Nguyen, H. T., & Tran, K. P. (2022). Light-weight federated learning-based anomaly detection for time-series data in industrial control systems. *Computers in Industry*, *140*, Article 103692. https://doi.org/10.1016/j.compind.2022.103692.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, *30*.

Wang, C. (2020). Iot anomaly detection method in intelligent manufacturing industry based on trusted evaluation. *The International Journal of Advanced Manufacturing Technology*, *107*(3), 993–1005. https://doi.org/10.1007/s00170-019-04274-0.

Wang, C., Wang, B., Liu, H., & Qu, H. (2020a). Anomaly detection for industrial control system based on autoencoder neural network. *Wireless Communications and Mobile Computing*, *2020*. https://doi.org/10.1155/2020/8897926.

Wang, Y., Perry, M., Whitlock, D., & Sutherland, J. W. (2020b). Detecting anomalies in time series data from a manufacturing system using recurrent neural networks. *Journal of Manufacturing Systems*. https://doi.org/10.1016/j.jmsy.2020.12.007.

Wang, S.-J., Cai, C. X., Tseng, Y.-W., & Li, K. S.-M. (2020c). Feature selection for malicious traffic detection with machine learning. In *2020 international computer symposium (ICS)* (pp. 414–419). IEEE.

Wang, X., Garg, S., Lin, H., Hu, J., Kaddoum, G., Piran, M. J., & Hossain, M. S. (2021a). Towards accurate anomaly detection in industrial Internet-of-things using hierarchical federated learning. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3074382.

Wang, H., Mumtaz, S., Li, H., Liu, J., & Yang, F. (2021b). An identification strategy for unknown attack through the joint learning of space–time features. *Future Generations Computer Systems*, *117*, 145–154. https://doi.org/10.1016/j.future.2020.11.023.

Wang, X., Garg, S., Lin, H., Hu, J., Kaddoum, G., Piran, M. J., & Hossain, M. S. (2021c). Toward accurate anomaly detection in industrial Internet of things using hierarchical federated learning. *IEEE Internet of Things Journal*, *9*(10), 7110–7119. https://doi.org/10.1109/JIOT.2021.3074382.

Wang, X., Pi, D., Zhang, X., Liu, H., & Guo, C. (2022). Variational transformer-based anomaly detection approach for multivariate time series. *Measurement*, *191*, Article 110791. https://doi.org/10.1016/j.measurement.2022.110791.

Wangwang, W., Yunchun, Z., Chengjie, L., Xuchenming, S., Yuting, Z., & Xin, Z. (2021). Network traffic oriented malware detection in iot (Internet-of-things). In *2021 international conference on networking and network applications (NaNA)* (pp. 301–307). IEEE.

Weinger, B., Kim, J., Sim, A., Nakashima, M., Moustafa, N., & Wu, K. J. (2022). Enhancing iot anomaly detection performance for federated learning. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.02.007.

Wu, D., Jiang, Z., Xie, X., Wei, X., Yu, W., & Li, R. (2019). Lstm learning with Bayesian and Gaussian processing for anomaly detection in industrial iot. *IEEE Transactions on Industrial Informatics*, *16*(8), 5244–5253. https://doi.org/10.1109/TII.2019.2952917.

Wu, Y., Dai, H.-N., & Tang, H. (2021). Graph neural networks for anomaly detection in industrial Internet of things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3094295.

Yang, H., Liang, S., Ni, J., Li, H., & Shen, X. S. (2020). Secure and efficient k nn classification for industrial Internet of things. *IEEE Internet of Things Journal*, *7*(11), 10945–10954. https://doi.org/10.1109/JIOT.2020.2992349.

Yang, K., Shi, Y., Yu, Z., Yang, Q., Sangaiah, A. K., & Zeng, H. (2022a). Stacked one-class broad learning system for intrusion detection in industry 4.0. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2022.3157727.

Yang, Y., Yang, X., Heidari, M., Khan, M. A., Srivastava, G., Khosravi, M., & Qi, L. (2022b). Astream: Data-stream-driven scalable anomaly detection with accuracy guarantee in iiot environment. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2022.3157730.

Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2020). Challenges and recommended technologies for the industrial Internet of things: A comprehensive review. *Measurement*, *151*, Article 107198. https://doi.org/10.1016/j.measurement.2019.107198.

Zeyu, H., Geming, X., Zhaohang, W., & Sen, Y. (2020). Survey on edge computing security. In *2020 international conference on big data, artificial intelligence and Internet of things engineering (ICBAIE)* (pp. 96–105). IEEE.

Zhan, P., Wang, S., Wang, J., Qu, L., Wang, K., Hu, Y., & Li, X. (2021). Temporal anomaly detection on iiot-enabled manufacturing. *Journal of Intelligent Manufacturing*, 1–10. https://doi.org/10.1007/s10845-021-01768-1.

Zhang, X., Li, J., Zhang, D., Gao, J., & Jiang, H. (2020). Research on feature selection for cyber attack detection in industrial Internet of things. In *Proceedings of the 2020 international conference on cyberspace innovation of advanced technologies* (pp. 256–262).

Zhou, X., Hu, Y., Liang, W., Ma, J., & Jin, Q. (2020). Variational lstm enhanced anomaly detection for industrial big data. *IEEE Transactions on Industrial Informatics*, *17*(5), 3469–3477. https://doi.org/10.1109/TII.2020.3022432.

Zugasti, E., Iturbe, M., Garitano, I., & Zurutuza, U. (2018). Null is not always empty: Monitoring the null space for field-level anomaly detection in industrial iot environments. In *2018 global Internet of things summit (GIoTS)* (pp. 1–6). IEEE.