IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 February 2024, accepted 22 April 2024, date of publication 29 April 2024, date of current version 10 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3395051

SURVEY

Anomaly Detection in Smart Environments: A Comprehensive Survey

DANIEL FÄHRMANN[1,2], LAURA MARTÍN[3], LUIS SÁNCHEZ[3], AND NASER DAMER[1,2], (Senior Member, IEEE)

[1]Fraunhofer Institute for Computer Graphics Research IGD, 64283 Darmstadt, Germany
[2]Department of Computer Science, Technical University of Darmstadt, 64283 Darmstadt, Germany
[3]Network Planning and Mobile Communications Laboratory, Universidad de Cantabria, 39005 Santander, Spain

Corresponding author: Daniel Fährmann (daniel.faehrmann@igd.fraunhofer.de)

This work was supported in part by German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE; and in part by Spanish State Research Agency (AEI) by means of the Project Semantically-Enabled Interoperable Trustworthy Enriched Data-Spaces (SITED) under Grant PID2021-125725OB-I00.

ABSTRACT Anomaly detection is a critical task in ensuring the security and safety of infrastructure and individuals in smart environments. This paper provides a comprehensive analysis of recent anomaly detection solutions in data streams supporting smart environments, with a specific focus on multivariate time series anomaly detection in various environments, such as smart home, smart transport, and smart industry. The aim is to offer a thorough overview of the current state-of-the-art in anomaly detection techniques applicable to these environments. This includes an examination of publicly available datasets suitable for developing these techniques. The survey is designed to inform future research and practical applications in the field, serving as a valuable resource for researchers and practitioners. It not only reviews a range of state-of-the-art anomaly detection methods, from statistical and proximity-based to those adopting deep learning-methods but also covers fundamental aspects of anomaly detection. These aspects include the categorization of anomalies, detection scenarios, challenges associated, and evaluation metrics for assessing the techniques' performance.

INDEX TERMS Anomaly detection, human activity recognition, machine learning, pattern recognition, safety.

I. INTRODUCTION

If a smart environment is considered a living human organism, where appliances, roads or machines, are its organs, then a smart environment should behave as an intelligent body. It knows when it's temperature exceeded the limit (e.g. home over heating) and it knows when the blood is flowing too slowly (e.g. traffic congestion). It knows how to keep all of its organs healthy and functioning at their best. Failure to detect or incorrect assumption of unhealthy situations could cause a loss of critical components that are necessary for its operation.

As for the health of the human body, similar principles apply to modern smart environments and their components, which are interconnected by modern Information and Communication Technology (ICT). In the course of the digital transformation, all kind of scenarios are becoming increasingly smart (e.g. smart homes, smart factories, smart roads, etc.). The term *Digital Transformation* refers to the use of digital technologies to transform traditional ways of doing business and delivering services [1]. Modern smart environments are now able to automatically gather knowledge about their environment and apply it according to the user's needs, a capability referred to as *Smart*. The term *Internet of Things* (IoT) refers to devices that are connected to the Internet and used to control and monitor an environment remotely [2]. IoT devices include various products embedded with processors, software, sensors (e.g., cameras, thermostats) and actuators (e.g., power switches, engines, valves, and pumps) that can be controlled and monitored remotely through a network connection.

Sensor technology is increasingly employed to quantify physical variables and accumulate data about human activities within ecosystems [3], [4], [5]. This technology

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Yu.

comprises various components specifically selected to align with the intended application and to ensure the enforcement of contemporary security standards. Moreover, nowadays, individuals are more and more utilizing personal sensors and wearable devices. This practice forms part of a trend known as the *Quantified Self*, which involves the self-measurement of personal physiological characteristics with the aid of wearable sensor technology [6]. Younger citizens are particularly inclined towards using devices like mobile phones [7] and fitness trackers [8] as tools to monitor and improve their health. These devices enable the user to measure various metrics, such as heart rate, the number of steps taken within a specific time interval, the number of calories burnt, as well as the localization and measurement of body movements. The scope of what can be monitored extends well beyond these examples. The abundance of sensors in smart environments enables the generation of large datasets that comprise various types of data. The availability of such rich datasets presents an exciting opportunity for the scientific community. It paves the way for the development of innovative algorithms designed to leverage this data, ultimately aiming to enhance the quality of life of people, the productivity of a factory or the traffic conditions.

Smart environments are composed of domains where people live and work. These domains might include entire cities, as well as smaller parts such as single buildings, homes, or infrastructures. Smart environments are designed with security and safety in mind [9], but it is still possible for unforeseen situations, failures or attacks to occur. Smart environments not only enable new opportunities for automated systems but also increase the need for solutions that can recognize hazardous situations [10]. IoT devices commonly have vulnerabilities that can be exploited by attackers. Therefore, the detection of unforeseen situations, failures or attacks in smart environments is crucial to prevent malicious consequences. Enhancing the possibilities of being accurately aware of the situations and processes in smart environments is important in order to reduce costs, damage to critical infrastructure, and threats to people within such environments.

Abnormal situations can be anything out of the ordinary. These situations include coordinated attacks, unwanted system behaviors (e.g., error states, malfunctions) or unforeseen situations that are recorded by monitoring sensors. Anomaly detection (AD) algorithms enable the detection of these situations and behaviors by recognizing anomalous patterns in sensory data.

AD and situation recognition are important tools for improving the safety and security of smart environments. AD refers to the process of identifying unusual or unexpected patterns or behaviors in data. Situation recognition, also known as event or scene understanding, involves using data from various sources to identify and understand the context of a situation. This can include recognizing patterns of behavior, determining the location and activities of individuals, and identifying objects or events that are relevant to the situation.

Together, AD and situation recognition can help to make smart cities more secure by providing early warning of potential security threats and enabling a more rapid and informed response to incidents. For example, a smart city's surveillance system might use AD to identify unusual patterns of activity in a particular area, and then use situation recognition to understand the context of the situation and determine an appropriate response. This might involve dispatching emergency services, issuing an alert to citizens, or taking other actions to address the threat.

There are several surveys on related topics, since the scientific community extensively reviewed AD [11], [12], [13], [14], [15], [16], [17], [18], [19], [20]. The landscape of AD research, has been extensively explored in these surveys. However, these surveys have adopted a more general perspective, focusing broadly on AD techniques without presenting the nuanced characteristics unique to individual smart environments. This overarching approach, while valuable, leaves a gap in the literature: a detailed understanding of how AD is tailored and applied to specific smart environments, namely smart home, smart transport, and smart industry, each with its distinct challenges and requirements. This survey addresses this gap by providing an essential resource for researchers and practitioners in the field. It goes beyond the general discussions of AD techniques and explores the specifics of how these techniques are applied in different smart environments. This focus is crucial as the dynamics and data characteristics of each environment vary significantly, influencing the choice and implementation of AD methods. This comprehensive approach enables researchers to gain a more informed understanding of which applications and research directions have been pursued in previous works, and what future directions might be most fruitful.

To this end, the contributions of this survey are as follows: First, we discuss smart environments, their application domains, and present a market analysis to show the increasing need for AD solutions. Second, we review on AD fundamentals in order to set the scenes on which kind of anomalies can exist on IoT time series, as well as, on how AD solutions have been typically assessed. The core contribution of this work is, indeed, the review on the advances in deep learning-based AD techniques compared with traditional techniques. In this regard, we review deep learning-based AD techniques and their applications in particular smart environments, including an analysis of commonly used sensor technologies and datasets utilized for the development and assessment of the proposed AD solutions.

The structure of this work is as follows: Section II introduces smart environments along with a market analysis. Section III presents an introduction to AD, including anomaly types, application scenarios, performance metrics, and development challenges. Section IV-A briefly categorizes traditional AD techniques. Section IV-B explores deep learning-based AD, providing a comprehensive overview of these techniques and their advantages. Section V investigates advancements in time series AD, discussing the utilization of deep learning models and their benefits and limitations. Section VI reviews datasets used for developing and evaluating AD algorithms. Section VII presents applications of AD in multiple smart environments. A discussion and future research directions are presented in Section VIII. Finally, this work concludes in Section IX.

II. BACKGROUND

This section briefly presents background on smart environments, and a market analysis regarding the increasing need for IoT-based technologies in these environments. Section II-A present background on smart environments and its components, to get an overview of the topic. Section II-B presents a market analysis of IoT-based technologies, with focus on the smart home, smart transport, smart industry, and smart energy environments that are discussed in this work.

A. SMART ENVIRONMENTS

Smart environments, in a broader sense, encompass smart cities as a subset. They are defined by the integration of advanced technologies, such as IoT, Artificial Intelligence (AI), and big data analytics, to enhance efficiency, sustainability, and habitability in various settings. Smart environments comprise interconnected smart objects within any living space, not limited to urban areas. According to Jakkula and Cook [21] a smart environment is "a system that collects data about the inhabitants of a living space and the environment in order to model and adapt the environment". This concept aligns with the IoT vision, as presented in [22]. The basic idea behind this vision is that various sensors and actuators can interact to achieve common goals. The key technologies that enable IoT are presented in their survey, alongside the IoT principal applications and future benefits.

Structurally, a smart environment is layered, comprising physical, communication, information, and decision layers [23]. The automation process in these environments can be conceptualized as a cyclical process involving three key stages: perception, reasoning, and action. During perception, the system utilizes sensors to collect data about the environment and identifies the current state in a bottom-up process. The sensors utilize physical components to monitor the environment and provide information through the communication layer. The gathered information is stored in a database in the information layer and processed into more useful knowledge by other information components, such as prediction or data mining mechanisms. In the reasoning stage, the system analyzes the current state by making use of decision making algorithms (e.g., rule engine) in the decision layer alongside predefined task goals and possible actions, thereby deciding on the optimal course of action. Finally, during the action stage, the system executes the selected action in a top-down manner. Once a decision is made, the services layers (information and communication) communicate the action to the physical layer. The physical layer utilizes physical components such as actuators to modify the state of the environment, and triggering a new perception stage [23].

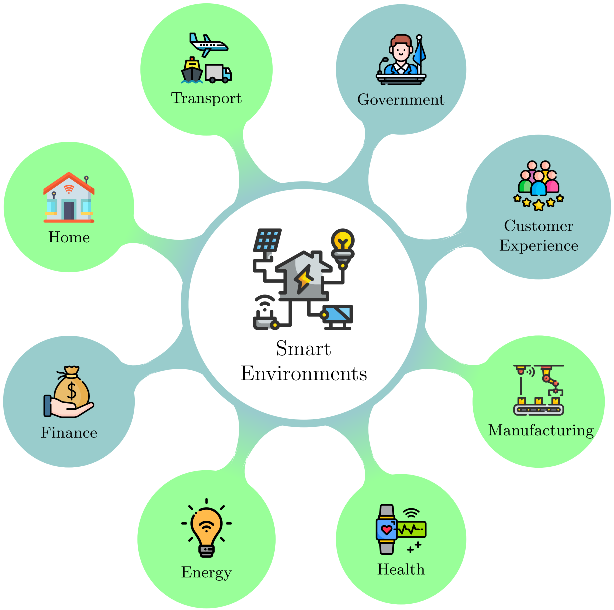


FIGURE 1. The best-funded smart environments in 2020. Anomaly detection applications in the green-colored smart environments are discussed in this survey.

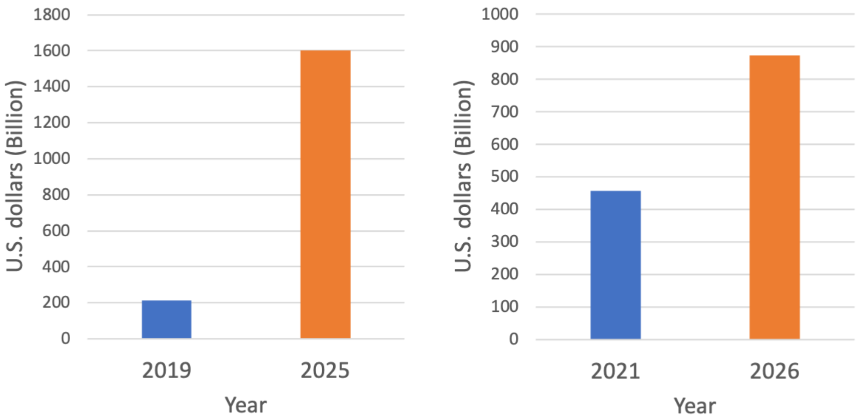
Figure 1 visualizes the most significant smart environments considering the estimated amount of IoT spending's in the year 2020 and the estimated amount of IoT spending's over the period 2014-2020. Most of the expenditures were made for smart finance, smart transport, smart government/environment, smart customer experience, smart health, smart homes, smart energy and smart manufacturing [2].

In this survey, we discuss applications of AD in key smart environments identified in [2], namely smart transport, smart manufacturing and smart energy, which we collectively term as "smart industry", as well as smart home and smart health, which we group under the term "smart home". We base this aggregation on shared features and integrative potentials that these environments possess.

B. MARKET ANALYSIS

This section presents a market analysis of IoT-based technologies in smart environments. The market for IoT-based technologies, especially in certain application domains, is growing rapidly. Homes with integrated health monitoring, intelligent transportation systems, automated manufacturing industries, and energy grid systems are some of the main areas where IoT-based solutions are expected to have the most impact, with a significant growth forecasted in the upcoming years.

According to the full-stack development company Softeq [24], there are indications that the declining demand for IoT solutions in the automotive, logistics and consumer



(a) Global market revenue for Iot [24].

(b) Global smart city market size [25].

FIGURE 2. The global IoT and smart city market is growing significantly.

electronics industries will be short-lived and that the digital transformation of traditional analog industries is more likely to accelerate. Figure 2 illustrates the estimated growth of the global market revenue for IoT-based technologies and the estimated growth of the smart city market. The forecast of the business data platform Statista [25] states that the global market revenue for IoT is expected to grow to 1600 billion U.S. dollars by 2025 as compared to 212 billion U.S. dollars in the year 2019. This indicates the accelerating demand for IoT-based technologies, underpinning the digital transformation. The revenue impact firm MarketsandMarkets [26] forecasts that the global Smart City market size will almost double from USD 457 billion in 2021 to USD 873.7 billion by 2026. This growth is driven by factors such as increasing urbanization, the need for sustainable and efficient cities, and advancements in technology. Regarding to the report, the major factors for the growth of the Smart Cities market are expected to be the demand for efficient transport, public safety, a healthy environment, and efficient energy consumption [27]. Another report by Zion Market Research [28] estimates that the global smart cities market will increase from \$1125 billion in 2021 to \$6050 billion in 2028, at a Compound Annual Growth Rate (CAGR) of 26%. This increases the need for solutions that enhance security and safety in the transportation, health and energy application domains.

IoT is a rapidly growing communication paradigm as the number of connected IoT devices is growing exponentially. The expected number of connected IoT devices by the year 2025 is 75.44 billion as compared to 30.73 billion in the year 2020 [29]. According to the market and consumer data company Statista, forecasts suggest that there will be around 50 billion IoT devices globally by 2030 [30].

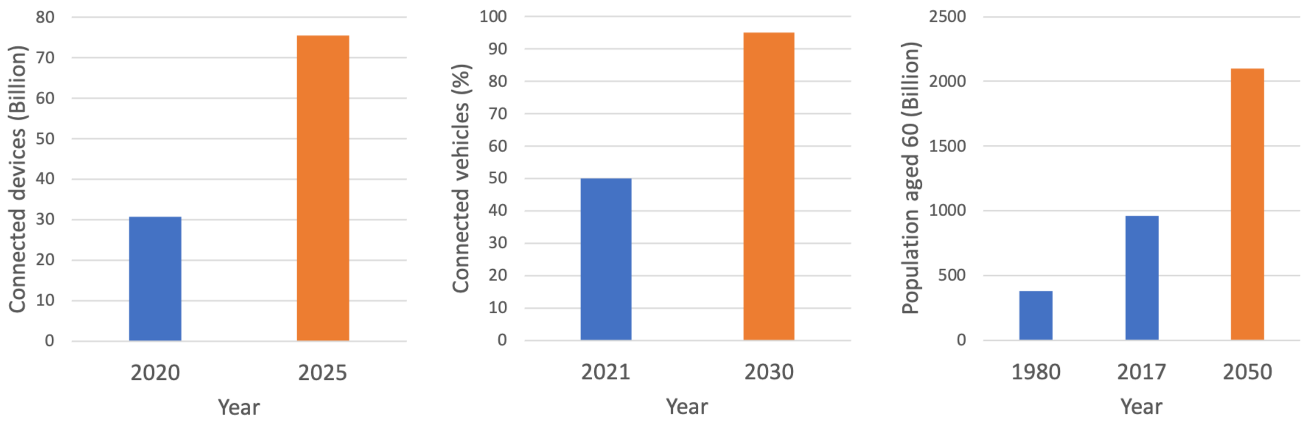
It is very important to guarantee security in the energy sector. This is emphasized by the National Intelligence Council (NIC) [31] that included IoT in the list of the six *Disruptive Civil Technologies* with potential impacts on U.S. national power.

Transportation will be increasingly automated and monitored remotely. The global management consulting firm McKinsey & Company reported that the number of new vehicles sold globally that will be connected to the Internet increases from around 50 percent in 2021 to about 95 percent in 2030 [32]. According to MarketsandMarkets Research, air transportation will have the largest impact on the smart transportation market in the period 2018–2023 [26]. In the smart building domain, emergency management will hold the largest market share. Smart cities in asia pacific regions are expected to hold the most significant market share because of their rapid adoption of smart technologies.

Health monitoring systems gain increasing attention. The Internet of Medical Things (IoMT) has risen in the recent years. In response to the COVID-19 pandemic, healthcare providers and digital health companies have progressively adopted IoMT solutions. Notably, the use of wearable devices has played a significant role in reducing the workloads of hospital staff and enhancing operational efficiency [33].

The number of elderly persons is also expected to grow rapidly. The Department of Economic and Social Affairs stated that the global population aged 60 years or more numbered 962 million in 2017, as compared to 382 million in 1980. Regarding to their report, the number of elderly persons is expected to reach 2.1 billion by 2050 [34]. The World Health Organization stated that by 2050, there will be 400 million people worldwide that are aged 80 years or more [35]. Monitoring the activities of elderly people at home remotely by making use of IoT-technologies and situation recognition algorithms can potentially decrease fatal consequences for the health of a city's inhabitants.

Industrial Internet of Things (IIoT) and automation have recently been seen as job killers in the factory. Today, manufacturers are turning to IIoT to remotely monitor equipment and production facilities. Situation recognition and AD algorithms help to prevent hazards to personnel or machinery, minimize downtime and save costs. Innovations in IIoT are being implemented with costs in mind. For the



(a) The expected number of connected IoT devices [29].

(b) Vehicles sold globally that will be connected to the Internet [30].

(c) Global population aged 60 years or more [31].

FIGURE 3. **IoT market analysis.**

industrial sector, this means equipping old machines with sensors, connectivity technologies, and cloud-based analytics such as AD solutions.

According to the NIC, IoT could contribute to the domestic economy and the military of the United States but also be a threat, since access to aggregated sensor data could be misused for criminal activities in the manufacturing domain.

The market analysis underscores a significant growth trajectory for IoT-based technologies, with a focus on sectors like health monitoring, intelligent transportation, and automated manufacturing. The expansion is marked by a rapid increase in the global market revenue for IoT. Key trends include the rising number of connected IoT devices and advancements in remote health monitoring and IIoT. These developments highlight the critical need for robust security measures in IoT implementations across various domains.

III. ANOMALY DETECTION

This section provides an introduction to AD in general. The fundamentals of AD are presented in Section III-A. Section III-B describes how different anomalies can be categorized. The learning scenarios in which AD techniques can be applied are presented in Section III-C. Section III-D presents the performance metrics typically used for evaluating AD solutions. Finally, Section III-E presents the challenges involved in the development of these solutions.

A. FUNDAMENTALS

Deep learning is a sub-field of machine learning that involves the use of neural networks to learn patterns in data. It has been widely applied in a variety of areas, including AD. The aim of AD (also referred to as outlier detection) is to identify instances that are dissimilar to others, such as instances that exhibit patterns significantly different from the underlying distribution of a dataset. The instances being dissimilar are called *anomalies*. According to [13], AD is the process of recognizing patterns that do not conform to the expected behaviour. AD has various applications, it is an important tool for credit card fraud detection [36], sensor network intrusion detection [37], fault detection [38], [39], fraud detection [40], medical diagnosis [41], human behaviour analysis [42], [43], computer network threat detection [44], [45] and many others.

Anomalies can be anything out of the ordinary. According to [46], outliers are also referred to as abnormalities, discordants, deviants, or anomalies in statistics and data mining literature. Previous work suggested various but similar definitions for anomalies. Traditionally, Hawkin [47] defined an anomaly by ''an observation which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism''. Barnett and Lewis [48] defined an anomaly by ''an observation (or subset of observations) which appears to be inconsistent with the remainder of that set of data''. A more modern view on AD is biologically inspired. In [49], the authors stated that expectation and surprise are the two factors in the human neural system that determine anomalies.

In fact, novelty detection is a related subject that aims at detecting previously unobserved patterns. Markou and Singh [50], [51] investigated statistical and neural network based novelty detection approaches. Novelty detection mechanisms are typically applied in scenarios where only the expected behaviour is known. Novelty detection algorithms also incorporate novel patterns into the detection mechanism after they have been detected, such that the mechanism covers the new notions of normalcy. Nonetheless, novelty detection algorithms are frequently applied to AD problems [13].

In general AD algorithms mainly work by estimating a model of normalcy based on data distributions. Anomalies are identified by measuring the probability that a test data sample is generated by the estimated model [50], [51].

Detecting anomalies in real-world applications involves several challenges. The AD algorithms that can be applied to a given scenario depend, for example, on data availability. The main difference between AD and many other statistical classification problems is that the data used to detect anomalies is inherently unbalanced. The fraction of labeled anomalous data instances is generally very low. Typically, it is not feasible to obtain a dataset that is labeled with all possible anomalies. Therefore, AD algorithms are usually divided into three different learning scenarios, depending on whether labeled data is available or not. Whether or not an observation is considered being anomalous also depends on the context in which the observation occurs. A high number of bicycle trips during summer is very likely, whereas during winter it is not. Another challenge is that AD methods typically produce a large amount of false alarms due to corrupt data or faulty sensors [13].

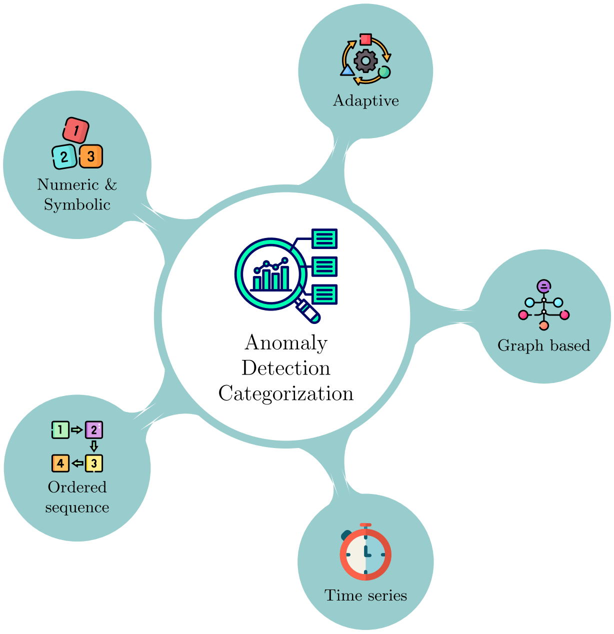


FIGURE 4. Categorization of previous work on AD algorithms.

Figure 4 illustrates a categorization of previous work on AD algorithms. The diverse landscape of AD has been extensively studied across various application domains, as highlighted in several surveys [11], [12], [13], [14], [15], [16], [17], [18], [52]. These surveys have discussed a wide range of approaches including numeric and symbolic outlier mining techniques [11], AD techniques for ordered sequences of events [14], time series data [15], and graph-based structures [16]. Adaptive AD models, which are particularly useful in dynamically changing environments, have also been covered [52]. The data distributions recorded in these environments are changing over time, such that AD algorithms developed for static datasets cannot be adequately applied in these environments. Other literature reviews cover comprehensive reviews and categorizations of AD techniques [12], [13], various deep learning based AD methods [17], and advancements in deep AD and key challenges involved [18]. This literature review, however, diverges fundamentally from existing surveys by concentrating on the application of AD algorithms within specific smart environments, namely smart homes, smart transport, and smart industry. Unlike general overviews of AD techniques as presented in [12] and [13], or focused discussions on deep learning-based methods in AD like the works of [17] and [18], this survey explores the practical implementation of these algorithms. The emphasis here is not solely on the technical sophistication of AD methodologies, but rather on their applicability and effectiveness in real-world smart environments. This includes an exploration of the interaction between AD solutions and the unique dynamics of IoT devices and sensor networks in smart homes, transportation systems, and industrial settings. The intricate balance between technological advancement and practical utility forms the cornerstone of this review, presenting a more application-oriented perspective on the field of AD within smart environments.

B. TYPES OF ANOMALIES

This section presents a commonly used categorization of anomaly types. According to Chandola et al. [13], anomalies can be categorized into three basic types: a) point anomalies, b) contextual anomalies, c) collective anomalies. Figure 5 visualizes examples for the three different anomaly types.

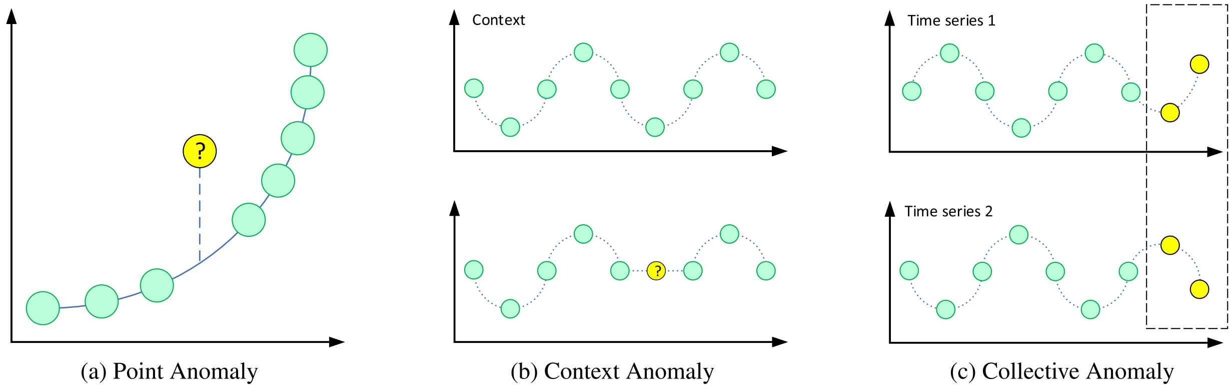
A point anomaly is a single data instance that significantly deviates from the remaining data instances (i.e. the data instance lies within a low-density region of values). Contextual anomalies depend on the context in which they occur. A contextual anomaly is a single data instance that deviates from the data instances given in the same context (i.e. the data instance is anomalous with respect to local values). The data instance might not be considered anomalous if another context is given. Last but not least, a collective anomaly refers to a group of data instances that are collectively considered anomalous. Even though the individual data instances in a collective anomaly may not be anomalous themselves, their occurrence together as a collection can be anomalous [13].

C. LEARNING SCENARIOS

This section presents common learning scenarios in which AD techniques are applied. Several works [13], [17], [53] investigated various AD techniques and their applications in detail and suggested to categorize AD techniques into three learning scenarios: a) supervised-, b) semi-supervised-, c) unsupervised- AD techniques. The learning scenarios are visualized in Figure 6. A brief description is given below.

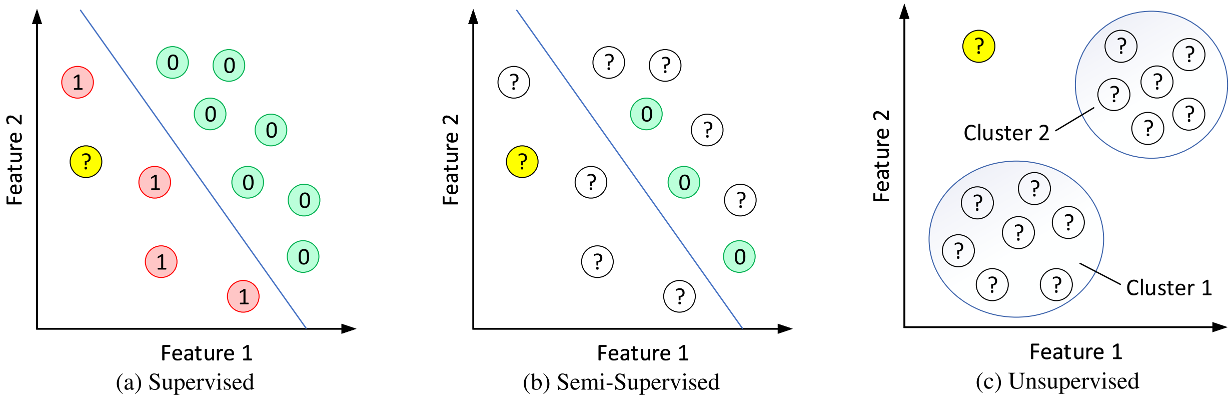
1) SUPERVISED

Supervised AD techniques are based on classifiers that categorize data instances into "normal" or "anomalous" instances. However, training classifiers in a supervised fashion requires training data that is annotated with ground truth labels [53]. Supervised AD approaches are suspect



(a) Point Anomaly (b) Context Anomaly (c) Collective Anomaly

FIGURE 5. Categorization of anomalies into three basic types, namely point anomalies, contextual anomalies, and collective anomalies [13]. The yellow and green spheres represent data instances of a dataset. Green spheres indicate normal data instances, while yellow spheres indicate anomalous data instances.



(a) Supervised (b) Semi-Supervised (c) Unsupervised

FIGURE 6. Categorization of AD techniques into three different learning scenarios, namely supervised, semi-supervised, and unsupervised learning. According to the models (blue lines) the data instances indicated by yellow spheres would be classified as negative (i.e. the data instance is anomalous). (a) Supervised learning involves training a model on positive (green spheres) and negative training examples (red spheres). (b) Semi-supervised learning only requires training examples that are annotated with one specific class label. In the illustration given above, only positive (i.e., normal) examples are provided in order to estimate the hypothesis function of the model. (c) In an unsupervised learning scenario, none of the training examples is annotated with a class label. Classification is achieved by grouping samples based on local density metrics, subsequently identifying anomalies as data instances residing in regions of low density.

to a common issue. The number of samples belonging to the "normal" class and the number of samples that are labeled "anomalous" in the training data is often imbalanced. Usually the number of anomalous samples in the training data is much lower compared to the number of normal samples [13], [17]. Typically, labeled real-world dataset that can be used for the development of AD algorithms are also very rare.

2) SEMI-SUPERVISED

Semi-supervised AD techniques require that the training data instances are entirely comprised of normal observations. A model of normalcy is estimated from the training data. The likelihood of a test instance being generated by the estimated model is used to identify whether a data instance is classified to be normal or anomalous. Observations that deviate from the learned model are classified as an anomaly. Far more semi-supervised methods exists in comparison to supervised methods, because semi-supervised methods are more widely applicable [13], [17], [53].

3) UNSUPERVISED

Unsupervised AD techniques do not rely on annotated data instances for model training. Instead, these techniques identify anomalous data instances based on the intrinsic properties of a dataset, meaning that they aim to learn the underlying distribution of the data automatically, and then use this knowledge to detect data instances that are most dissimilar to the majority of instances [13], [17], [53].

D. EVALUATION METRICS

This section briefly presents evaluation metrics commonly used for AD techniques. The evaluation of AD techniques is crucial to assess their performance and complexity to compare different methods. The choice of the metrics can have a significant impact on the results of the evaluation.

1) PERFORMANCE METRICS

a: PRECISION

The precision (also called positive predictive value) represents the fraction of actual positives among the instances

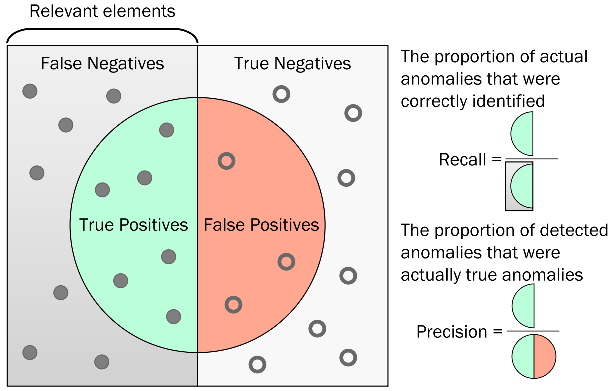

Relevant elements
False Negatives
True Negatives
True Positives
False Positives
The proportion of actual anomalies that were correctly identified
Recall =
The proportion of detected anomalies that were actually true anomalies
Precision =

FIGURE 7. The Precision and Recall metrics [54].

classified as positive by the model. In the context of AD, precision quantifies the proportion of data points correctly identified as anomalies out of all the instances that the detection algorithm flags as anomalies. Essentially, it measures the accuracy of the algorithm in classifying anomalies, or in other words, how often the instances flagged as anomalies are indeed actual anomalies. However, it is important to note that precision does not give any information regarding the anomalies that the algorithm failed to detect. This limitation can be addressed by considering recall alongside precision to have a more comprehensive understanding of the algorithm's performance. The precision is given by Equation (1) and visualized in Figure 7.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

b: RECALL

The recall is the fraction of actual positives that are correctly identified by the model. In the context of AD, the recall rate refers to the proportion of actual anomalies that are identified by the anomaly detector. It is essential to recognize that recall does not take into account false positives, i.e., normal instances incorrectly classified as anomalies. As such, a naive detector that labels every instance as an anomaly will achieve a recall of 100%, but this isn't practically useful as such a detector would fail to distinguish between normal and anomalous instances. The recall is given by Equation (2) and visualized in Figure 7.

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

c: F1-SCORE

The F1-Score measure is the harmonic mean of precision and recall [55] and is often used as a overall performance metric. It is necessary to balance between precision and recall, especially if a large number of true negative (i.e. normal instances) exists. The F_1 measure is given by Equation (3).

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} = \frac{TP}{TP + \frac{1}{2}(FP + FN)} \tag{3}$$

d: TRUE POSITIVE RATE (TPR)

The TPR indicates the number of correctly classified anomalies among all anomalies. Recall and TPR are essentially the same in the context of evaluating classification models in machine learning. The TPR follows the same formula and is given by Equation (4).

$$TPR = \frac{TP}{TP + FN} \tag{4}$$

e: FALSE POSITIVE RATE (FPR)

The FPR refers to the number normal data instances that where mistakenly classified anomalous. The FPR is given by Equation (5).

$$FPR = \frac{FP}{FP + TN} \tag{5}$$

f: TRUE NEGATIVE RATE (TNR)

The TNR represents the number of correctly classified normal data instances. The TNR is given by Equation (6).

$$TNR = \frac{TN}{TN + FP} \tag{6}$$

g: FALSE NEGATIVE RATE (FNR)

The FNR refers to the number anomalies that where mistakenly classified normal. The FNR is given by Equation (7).

$$FNR = \frac{FN}{FN + TP} \tag{7}$$

h: RECEIVER OPERATING CHARACTERISTIC (ROC)

The ROC curve is a commonly used metric that reflects the performance of a binary anomaly detector.

i: AREA UNDER THE CURVE (AUC)

The AUC, specifically for the ROC curve, is a commonly used evaluation metric to assess the model's ability to differentiate between classes [56]. It represents the likelihood that a randomly selected anomaly is assigned a higher score by the model compared to a non-anomaly instance [57].

2) COMPLEXITY METRICS

Apart from the commonly used performance measures, it might be relevant to asses the efficiency of the detection algorithm depending on the application. For example, if the detection algorithm should run on an embedded device with limited computational and storage capabilities, it might be important to asses the algorithm in terms of time, computational, and storage complexity.

a: COMPUTATIONAL COMPLEXITY

This measure evaluates the computational resources required by the algorithm to complete the task.

b: MULTIPLY-ACCUMULATE (MAC)

A MAC operation is a mathematical calculation used in many areas of science and engineering, particularly in digital signal processing and machine learning. It is a simple and efficient operation that involves multiplying two numbers and then adding the result to an accumulator, which is a register that stores a running total. This operation is given by Equation (8).

$$a \leftarrow a + (b \times c), \tag{8}$$

where a is the accumulator, b and c are numbers.

c: FLOATING POINT OPERATIONS (FLOPS)

FLOPs are a standard measure of computational complexity and represent the number of arithmetic operations (additions and multiplications) required to perform a computation. The number of FLOPs required for a forward pass through a neural network depends on the number and kind of layers, neurons, and activation functions in the model. To compute the total number of FLOPs required for a forward pass through a neural network, we can sum up the FLOPs for each layer and activation function in the model. Similarly, to measure the time complexity of a backward pass through the model (i.e., computing gradients with respect to the model parameters), we can count the number of FLOPs required for each layer and activation function.

d: STORAGE COMPLEXITY

This measure evaluates the storage requirements of the algorithm. The storage complexity of a deep neural network can be measured by estimating the total number of parameters or weights required to store the model. These parameters represent the learnable components of the model, and determine the model's capacity. The storage complexity of a neural network is computed by counting the number of parameters in each layer, which depends on the layer's type and configuration. An important factor in determining the storage complexity is the precision of these parameters. For example, if the model uses 32-bit floating-point numbers (FP32), each weight or bias would require 32 bits of storage. The choice of precision, such as FP32, FP16, or even lower precision formats, directly impacts the total memory footprint of the model. Lower precision formats can significantly reduce storage requirements at the expense of potential losses in predictive performance. To compute the total storage complexity, the parameter counts across all layers are summed. This cumulative figure represents the model's storage complexity. The consideration of the storage complexity is especially critical for deployment in environments with limited storage capacity, such as mobile or embedded devices.

e: TIME COMPLEXITY

This measure evaluates the time required by the algorithm to complete the task. The time complexity of a deep neural network refers to the amount of time required to perform a forward or backward pass through the network on a single input example. It depends on the number of operations required to compute the output and the gradients of the model, as well as the size and structure of the model. To measure the time complexity of a deep neural network, we can count the number of Floating Point Operations (FLOPs) required to compute the output and gradients of the model for a single input example. It's important to note that while the theoretical time complexity measured in FLOPs is hardware-independent, the actual time taken to execute these operations can vary significantly based on the hardware's capabilities. Faster processors or specialized hardware like GPUs can perform these operations more quickly than less capable hardware. Therefore, while the number of FLOPs as a theoretical construct remain constant, the practical execution time is indeed influenced by the hardware used.

E. CHALLENGES

This section presents typical challenges involved in AD. Section III-E1 presents challenges typically encountered when dealing with AD in smart environments. Section III-E2 focuses on challenges specific to time series data. Section III-E3 examines challenges regarding the evaluation of AD algorithms. Section III-E4 describes privacy and user acceptance concerns.

1) SMART ENVIRONMENTS ANOMALY DETECTION CHALLENGES

This section presents the challenges typically encountered in AD. Detecting anomalies in smart environments is a challenging task, as it involves complex dynamics such as traffic, social, and operational dynamics [58]. Addressing these challenges can lead to the development of effective AD methods that can enhance situational awareness and improve decision-making processes. In this work, we categorize the challenges involved in AD into five categories: scarcity, complexity, integration, granularity, and contextualization challenges. We provide a description of each category below.

a: SCARCITY

The scarcity of annotated anomalous events in datasets is a major challenge in AD, making it difficult to detect these events directly [59], [60]. Anomalies are typically rare occurrences in comparison to normal events, resulting in highly imbalanced datasets. Moreover, in many cases, the deviation of an anomalous event from normalcy cannot be measured accurately since the true data distributions cannot be estimated based on scarce observations [61]. Manually labeling data instances is often a time-consuming and expensive process, primarily because human supervision is required. Supervised methods are likely to overfit due to the imbalance of normal and anomalous events in labeled training data [62], making it necessary to employ other approaches, such as unsupervised methods that do not rely on labeled training data.

b: COMPLEXITY

The complexity of data is another major challenge. The influence factors of anomalous events in smart environments can

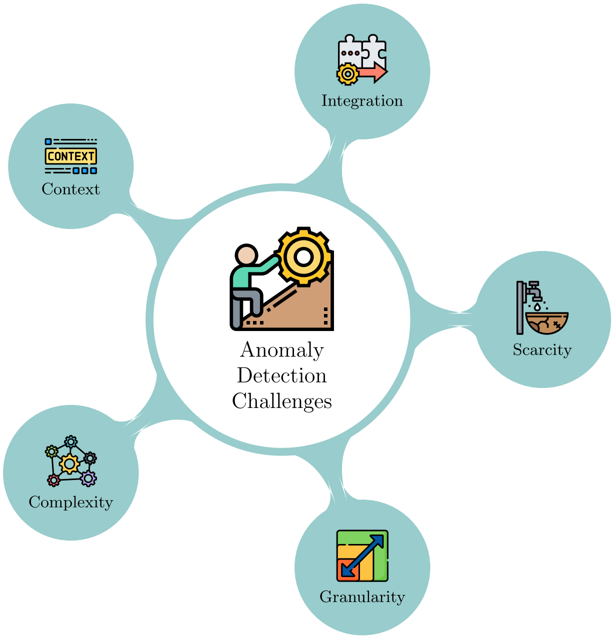


FIGURE 8. The challenges involved can be categorized as follows: a) scarcity, b) complexity, c) integration, d) granularity, and e) contextualization.

be spatial (e.g., region-specific traffic flow) or temporal (e.g., weather, time) in nature [59]. AD algorithms must be able to consider multiple data sources and different combinations of changes between these data sources to compute the degree of abnormalcy [60], [63]. High-dimensional data can lead to computational difficulties and hinder the performance of AD algorithms. Distance-based AD algorithms typically perform poorly in high dimensions due to distance concentration [64]. Additionally, the size of the data is important since the AD algorithms applied must potentially be scalable to very large datasets. Today's data-centric ecosystems are focal points of extensive data accumulation. Smart traffic systems, for example, are a hub of high-dimensional data, integrating real-time inputs from countless sensors, cameras, and GPS systems. These inputs, ranging from vehicle telemetry to public transportation utilization patterns, aggregate to form extensive datasets.

c: INTEGRATION

The integration of spatio-temporal data from multiple sources, and different data formats such as structured (e.g., weather history) and unstructured data (e.g., citizen complaints) raises the challenge of data integration [59], [60]. The data may also originate from different domains, and their distributions and scales may deviate [61], leading to challenges like domain adaptation.

d: GRANULARITY

The spatial and temporal granularity of data can significantly impact AD performance. Probabilistic methods typically do not perform well on highly granular data due to the high noise-to-signal ratio inhibiting the detection of characteristic patterns [65]. Therefore, it is important to find an appropriate balance between the level of granularity and the data quality. There are multiple possibilities for combining spatial and temporal information, making it a challenging task to determine the most suitable granularity for detecting anomalies [61]. Consequently, determining the optimal level of granularity for a given application is an important research direction.

e: CONTEXTUALIZATION

To infer the context in which events take place and differentiate anomalous from normal events under the given conditions, the complex relationships between the influence factors must be considered [60], [63]. The criteria for anomalies under certain conditions differ and must be defined. Previous work often assumes the data is independent and identically distributed, whereas in reality, data dependencies exist that need to be integrated into the AD model for effective detection [60]. Figure 9 visualizes the contextualization challenges. For instance, when dealing with time series, temporal data dependencies must be considered. In the case of images, spatial dependencies between pixels need to be taken into account. Urban transportation networks can be naturally represented by graph-like structures, requiring relational dependencies to be considered in the detection process.

2) TIME SERIES ANOMALY DETECTION CHALLENGES

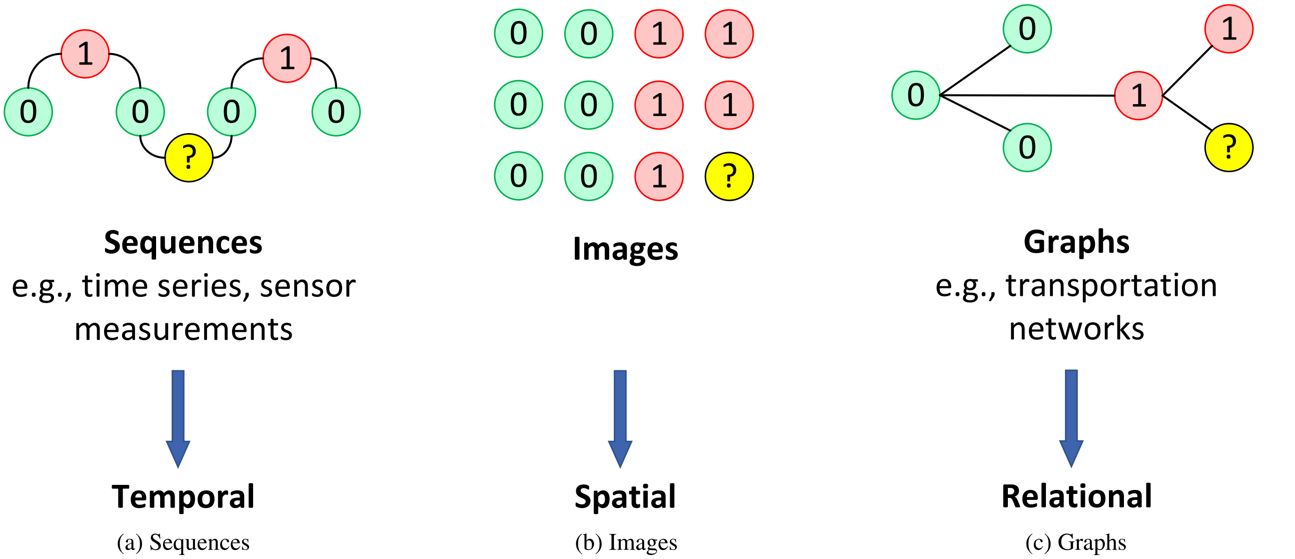
This section presents the challenges typically encountered in time series AD. Time series AD involves identifying unusual or unexpected patterns in temporal data. While many challenges in time series AD are common to AD in general, some are unique or more prominent in time series data. The time series challenges identified in this work are visualized in Figure 10 and briefly described below.

a: NON-STATIONARITY IN TIME SERIES DATA

Time series data, such as traffic patterns and driving behavior, are inherently non-stationary, with their statistical properties changing over time. This non-stationarity is further exacerbated by external disruptions, such as pandemics. For instance, the COVID-19 pandemic significantly altered traffic dynamics in cities like New York. Traditional AD methods often assume stationarity in the data, making them less effective in such environments where historical data may no longer be representative of the current state. This necessitates the development of adaptive algorithms capable of adjusting to these evolving patterns in order to maintain accuracy in AD [66].

b: SEASONALITY AND TRENDS

Many time series data sources come with seasonal and long-term shifts [67], [68], [69]. These temporal elements can significantly influence individual observations, necessitating



(a) Sequences (b) Images (c) Graphs

FIGURE 9. Contextualization challenges that need to be considered in the AD process. Effective AD requires considering temporal, spatial, or relational data dependencies. The contextualization challenges are shown for (a) sequences, (b) images, and (c) graphs.

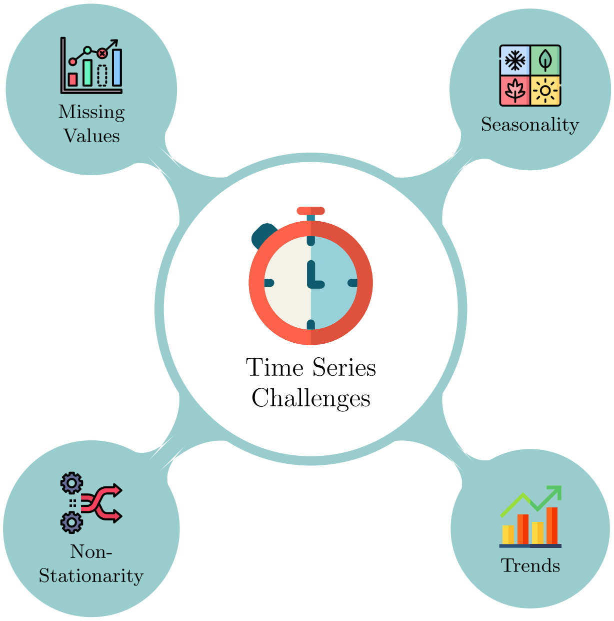


FIGURE 10. The challenges involved in time series AD can be categorized as follows: a) seasonality and trends, b) non-stationarity, c) varying data quality, and d) noise.

a nuanced approach in AD. It becomes imperative to consider both the current seasonality and overarching trends to accurately discern anomalies. This requirement adds complexity to the process, as it involves differentiating between typical periodic variations and genuine anomalies [69]. The determination of an anomalous temperature measurement depends on both seasonal variations and long-term trends [70]. This highlights the need to adjust thresholds for anomaly detection depending on temporal factors, recognizing that what constitutes an anomaly is not static but varies depending on the environmental and temporal context.

c: MISSING VALUES

Time series data frequently contain missing values, which pose a significant challenge in AD. This issue can arise from various factors such as sensor malfunctions, irregularities in data recording or synchronization issues, especially when sensors record data at different timestamps [71], [72], [73]. Handling missing values is critical because inadequate treatment can disrupt the temporal structure of the data and potentially introduce bias, leading to misleading results. One common approach to address missing values is interpolation, where values are estimated and filled in based on the neighboring data points. This process, however, must be executed with caution, as improper interpolation can sometimes distort the underlying patterns and trends in the time series, adversely affecting the performance of the algorithm. Thus, it is essential to employ appropriate methods for handling missing values that take into consideration the temporal dependencies and characteristics of the time series data [73].

3) EVALUATION CHALLENGES

This section presents the challenges typically encountered when evaluating AD methods. Some challenges are specifically related to the evaluation of AD algorithms, rather than the process itself. Figure 11 visualizes the challenges. These evaluation-related challenges include:

a: LACK OF GROUND TRUTH

In many real-world scenarios, it is difficult to obtain labeled data indicating whether a data point is an anomaly or not. This lack of ground truth makes it hard to evaluate the performance of the algorithms and compare them to alternative methods. This challenge is specific to evaluation, as it involves the difficulty in obtaining labeled data indicating whether a data

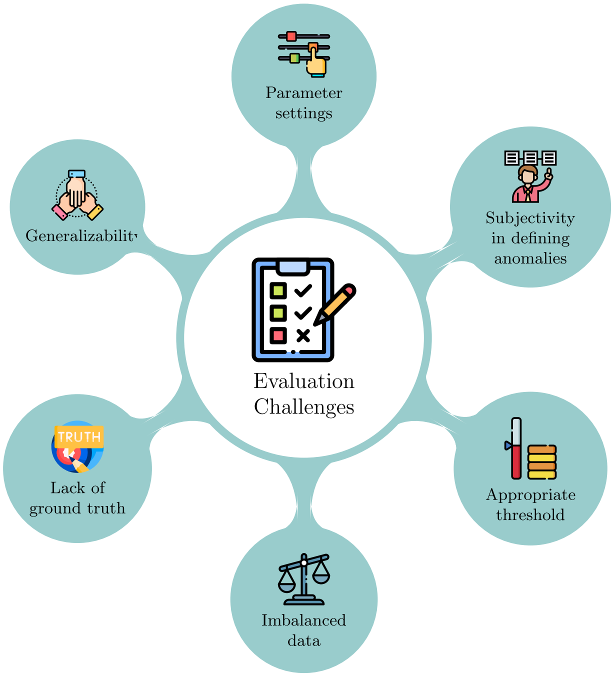


FIGURE 11. The challenges involved in the evaluation of AD algorithms.

point is an anomaly or not, which is necessary for assessing the performance of an algorithm. However, training a model is possible without ground truth labels, using unsupervised methods [74].

b: IMBALANCED DATA

Anomalies are, by definition, rare events. This results in highly imbalanced datasets where the number of normal instances far exceeds the number of anomalous instances [60]. Standard evaluation metrics, like accuracy, may not be suitable for imbalanced data, as a high accuracy can be achieved by merely classifying all instances as normal. Alternative metrics like precision, recall, F1-score, and AUC may be more appropriate in such cases [74], [75]. While imbalanced data is a common characteristic of AD problems, the challenge of choosing appropriate evaluation metrics to account for the imbalance is specific to the evaluation process.

c: APPROPRIATE THRESHOLD

AD often involves setting a threshold to distinguish between normal and anomalous data points. Choosing an appropriate threshold can be challenging, as it may depend on domain knowledge or the specific goals of the analysis. The choice of threshold can significantly impact evaluation metrics and the perceived performance of the algorithm [75]. Although setting a threshold is often part of the process, determining an appropriate threshold to assess algorithm performance and compare different methods is a challenge unique to evaluation.

d: SUBJECTIVITY IN DEFINING ANOMALIES

The definition of an anomaly can be subjective and may vary depending on the application or domain. This subjectivity can make it difficult to consistently evaluate and compare different algorithms. The challenge of subjectivity in defining anomalies is related to evaluation because it affects the consistency and reliability of performance assessments and comparisons between different algorithms [76].

e: SENSITIVITY TO PARAMETER SETTINGS

Many algorithms require the selection of parameters or hyperparameters. The performance of these algorithms can be highly sensitive to the chosen settings, making it challenging to ensure a fair comparison between different methods.

f: GENERALIZABILITY

AD algorithms may perform well on a specific dataset or within a particular domain but fail to generalize to other datasets or domains. Evaluating the generalizability of an algorithm can be challenging, as it requires testing across diverse settings [76], [77].

4) PRIVACY AND USER ACCEPTANCE CONCERNS

This section focuses on the privacy and user acceptance concerns associated with AD in smart environments. The growing reliance on data-driven methods and the increasing availability of data make techniques more effective and valuable. However, as smart environments rely on the collection and analysis of large amounts of personal data, privacy and user acceptance are crucial issues that need to be addressed for successful deployments. In the context of this review on privacy and user acceptance concerns, the term "users" refers to the individuals or groups who interact with or are affected by the smart environments that employ the AD systems. These users might encompass a broad range of individuals. The user acceptance concerns that are described in the following are particularly important to the residents or occupants of smart environments, as they are the primary group whose personal data is being collected and analyzed, and who are most directly affected by potential issues like sensitive data exposure, identification risk, perceived intrusiveness, false positives/negatives, and loss of autonomy and control. The residents or occupants are the individuals living or working in spaces where the smart environments are implemented. This group might include homeowners in smart homes, employees in smart industrial environments, or residents in smart cities. The concerns and mitigations identified in this work are geared toward the concerns of this group. Figure 12 visualizes the concerns and mitigations, a brief description is provided below.

a: PRIVACY CONCERNS

Sensitive Data Exposure: AD often requires the collection and analysis of sensitive information, such as personal [78] or

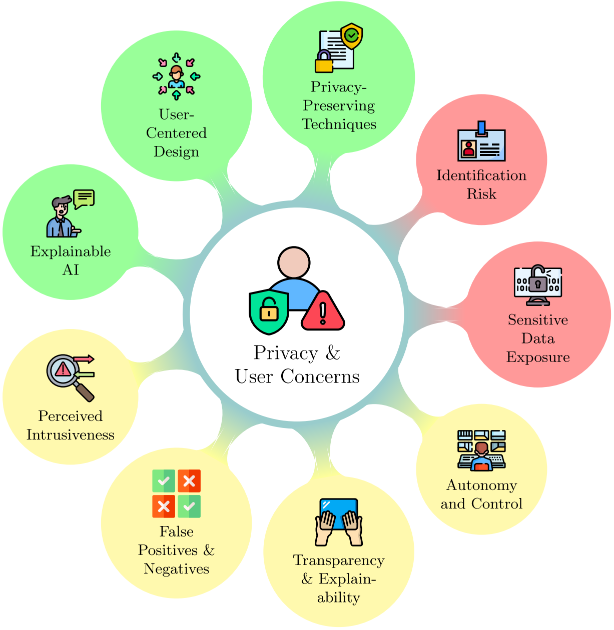


FIGURE 12. Concerns and mitigation strategies associated with AD. The privacy concerns, mitigation strategies, and user acceptance concerns are colored in red, yellow, and green respectively.

financial data [79]. Unauthorized access to this information may lead to privacy breaches and potential harm to individuals or organizations.

Identification Risk: Anonymization techniques are commonly used to protect individual privacy. However, sophisticated adversaries may still be able to re-identify individuals by linking anonymized data with other publicly available information, posing privacy risks [80], [81].

b: USER ACCEPTANCE CONCERNS

Perceived Intrusiveness: Users may perceive AD systems as intrusive or invasive, especially when these systems monitor personal behavior or require access to sensitive information. This perception can negatively affect user acceptance and adoption.

False Positives and Negatives: AD algorithms may produce false positives (identifying normal instances as anomalies) or false negatives (failing to identify actual anomalies). Such inaccuracies can lead to significant frustration and mistrust among users, directly undermining their acceptance of the system [82]. However, accurately identifying and analyzing these instances of false positives and negatives is crucial, as it provides valuable feedback for the optimization of the AD algorithm.

Transparency and Explainability: The lack of transparency and explainability in some methods, particularly those based on complex machine learning models, can hinder user acceptance. Users may be reluctant to trust systems they do not understand or cannot easily interpret [83], [84].

Autonomy and Control: Users may feel a loss of autonomy and control when automated systems are introduced, especially if these systems make decisions or take actions without user input or oversight. This loss can contribute to resistance and decrease user acceptance [85].

Mitigation Strategies: Privacy and user acceptance are critical considerations in the deployment of AD techniques. Addressing these concerns requires a multidisciplinary approach that considers technical, ethical, and social aspects. Future research should continue to explore innovative methods for preserving privacy while maintaining the effectiveness and fostering user acceptance through transparency, communication, and user-centered design.

Privacy-Preserving Techniques: Researchers can develop and employ privacy-preserving techniques, such as differential privacy and secure multi-party computation, to minimize privacy risks [86], [87].

User-Centered Design: AD systems should be designed with user needs and preferences in mind. Involving users in the design process and incorporating their feedback can help address user acceptance concerns [85].

Explainable AI: Developing explainable and interpretable algorithms can enhance user trust and acceptance by providing insights into the system's decision-making process [83], [84].

IV. ANOMALY DETECTION TECHNIQUES TAXONOMY

Among the different solutions that have been proposed for AD, it is possible to distinguish two big categories. The first works working on AD employed traditional statistical, proximity, and deviation-based mechanisms to identify anomalies. However, more recently, the advances in machine learning have opened new alternatives based on deep learning algorithms. In the following sub-sections both approaches are reviewed, providing an outlook on the alternatives for each of them, as well as, which are their main limitations.

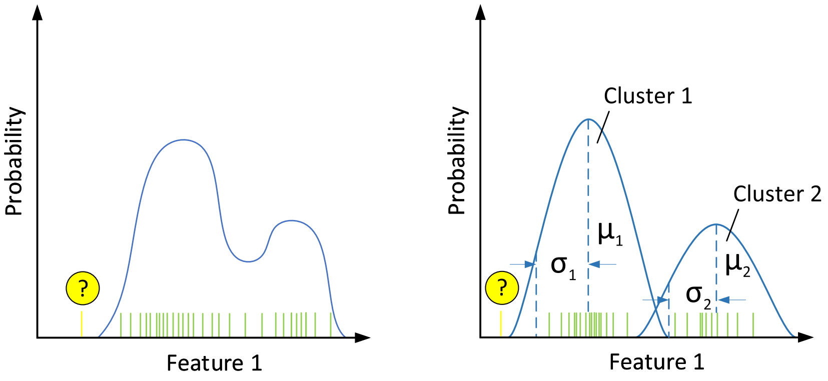
A. TRADITIONAL ANOMALY DETECTION

This section presents traditional AD techniques. Previous works categorized traditional techniques into statistical, proximity and deviation based methods [53]. Hereunder, a more detailed description of the categories is provided, including key examples of the techniques belonging to each category.

Statistical Anomaly Detection: Methods that assume data is generated by probability distributions and identify anomalies as data instances that deviate significantly from the expected distribution. Examples include Gaussian Mixture Models (GMMs) [88] or kernel density estimation [89].

Proximity Anomaly Detection: Methods that identify anomalies as data instances that are isolated from the majority based on their distance, density, or clustering [90]. Examples include k-Nearest Neighbors (kNN) [91], Local Outlier Factor (LOF) and DBSCAN [92].

Deviation-Based Anomaly Detection: Methods that identify anomalies as data instances that have a significant deviation from the expected distribution or subspace structure.



(a) Kernel density estimation

(b) Mixture of gaussians

FIGURE 13. Statistical AD techniques. (a) Kernel density estimation estimates the probability density function of a random variable in a non-parametric fashion. (b) A gaussians mixture model is comprised of several Gaussians, where each Gaussians is parameterized by its mean μ and its variance σ.

Examples of algorithms that can be used for deviation-based include PCA [93] and subspace-based methods like Low-Rank Representation [94].

1) STATISTICAL ANOMALY DETECTION

Statistical AD methods assume that data is generated by probability distributions. The probability distributions are defined by either parametric models (e.g. mixture of gaussians [95]) or non-parametric models (e.g. kernel density estimation [89]). Anomalies are identified as data points that deviate significantly from the probability distribution (i.e. the probability that a data point is generated by the model is low). One advantage of statistical AD methods is that they are theoretically justifiable and objective, as they provide probabilities to determine whether a data instance is anomalous [90]. However, the performance of these methods heavily depends on the choice of model and its parameters. Figure 13 visualizes basic statistical models, a brief description is provided below.

a: KERNEL DENSITY ESTIMATION

Kernel density estimation is a non-parametric method for estimating the probability density function of a random variable. It estimates the probability density of a point by convolving the point with a kernel function. The bandwidth of the kernel function determines the width of the distribution and hence, the sensitivity of the method to anomalies. Figure 13a shows an example of kernel density estimation.

b: MIXTURE OF GAUSSIANS

Mixture of Gaussians is a parametric method that models the data as a combination of several Gaussian distributions. Each Gaussian distribution is parameterized by its mean μ and variance σ. The method then calculates the likelihood of a data point being generated by each Gaussian and uses these probabilities to determine whether the point is anomalous. Figure 13b shows an example of mixture of Gaussians.

c: OTHER STATISTICAL METHODS

Other statistical methods for AD include confidence intervals and regression analysis. These methods can be used to identify outliers in univariate or multivariate data by comparing them to the expected distribution.

d: LIMITATIONS

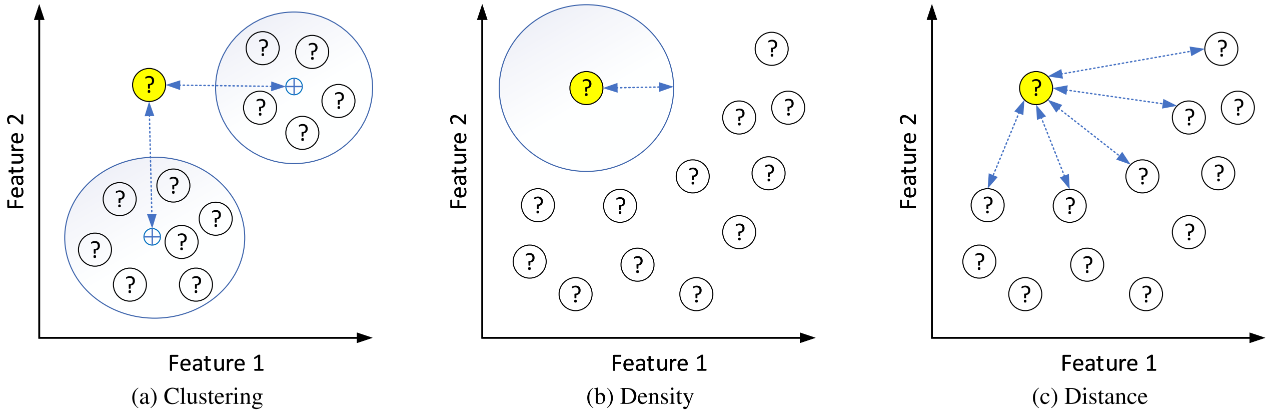
One of the main limitations of statistical AD methods is that they assume that the data is generated by a stationary and well-defined probability distribution. In real-world scenarios, the distribution may change over time, making it challenging to detect anomalies. Additionally, the choice of model and its parameters can heavily influence their performance. It is crucial to carefully make a selection of the appropriate method and evaluate its effectiveness for a given problem.

2) PROXIMITY ANOMALY DETECTION

Proximity-based AD algorithms identify anomalous data instances that are isolated from the majority. These methods are based on the assumption that normal data instances are dense and form clusters, while anomalies are isolated or form small clusters. According to [90], Proximity-based AD algorithms can be broadly categorized into clustering-based, density-based, and distance-based methods. The fundamental working principles of these methods are visualized in Figure 14. Clustering-based methods identify anomalies as data points distant from cluster centroids, while density-based methods flag anomalies in low-density regions compared to neighbors. On the other hand, distance-based methods consider data points with large distances to neighbors as anomalies.

a: CLUSTERING-BASED METHODS

Clustering-based methods involve clustering the data and identifying anomalous data instances as those that do not belong to any cluster or belong to a small one. In order to detect anomalous data points, the distance of a data point to



(a) Clustering (b) Density (c) Distance

FIGURE 14. Proximity based AD algorithms identify anomalous data instances that are isolated from the majority. Anomalies can be detected this way using three different approaches: a) clustering based, b) density based, c) distance based [90].

the cluster centroids (as in Figure 14a) or alternatively, the size of the closest cluster is evaluated [52], [90].

b: DENSITY-BASED METHODS

Density-based methods measure the local density of data instances and identify anomalies as those that have a lower density than their neighbors. For example, if a particular data point lies in a sparse region (i.e. the number of data points within a local region is below a threshold, as in Figure 14b), the data point is considered to be anomalous [90].

c: LOCAL OUTLIER FACTOR (LOF)

The LOF algorithm [96] measures the degree of a data point being an outlier, depending on how isolated the data point is in respect to its local neighborhood. LOF calculates the local density of a data instance and compares it to the local densities of its neighbors.

d: DENSITY-BASED SPATIAL CLUSTERING OF APPLICATIONS WITH NOISE (DBSCAN)

DBSCAN [97] is a density-based clustering algorithm that can also be used for AD. In DBSCAN, data instances that are not in a dense region are considered anomalous.

e: HIERARCHICAL SPATIAL CLUSTERING OF APPLICATIONS WITH NOISE (HDBSCAN)

In [98], Campello et al. suggested an integrated framework for density-based cluster analysis. The HDBSCAN algorithm the authors proposed, aims at a complete clustering hierarchy with varying densities. The authors suggest using the resulting hierarchy to assign a normalized outlier score to the clusters regarding their global and local neighborhood. The proposed clustering algorithm can also be used in semi-supervised learning scenarios by taking user annotated constraints into consideration.

f: LIMITATIONS

A limitation of proximity-based AD methods is that they assume that normal data instances are dense and form dense clusters, while anomalies are isolated or form small clusters. However, in real-world scenarios, anomalies may not be isolated or may form dense clusters, making it challenging to detect them using these methods.

g: DISTANCE-BASED METHODS

In distance-based methods, for example, the k-Nearest Neighbor, distances for a particular data point can be evaluated (as in Figure 14c), and an anomaly is detected if the k-Nearest Neighbor distances are large [90]. Distance-based methods are effective in detecting both global and local anomalies but may be sensitive to the choice of the distance metric and the value of k.

3) DEVIATION-BASED ANOMALY DETECTION

Deviation-based AD methods are based on the assumption that anomalies have a larger deviation from the normal data instances in some feature space. These methods generally involve two steps: (1) obtaining a low-dimensional representation of the data using a spectral decomposition approach, and (2) comparing the reconstructed data or reduced space to the original data to obtain a deviation score. Anomalies can be identified as data instances that have a high deviation score [90].

a: RECONSTRUCTION-BASED METHODS

Reconstruction-based deviation methods involve obtaining a low-dimensional representation of the data and then reconstructing the original data instances from their lower dimensional representations. The deviation between the original data instances and their reconstructions serves as an anomaly score, with anomalous data instances having a high reconstruction error. Instead of computing reconstruction errors by reconstructing the original data from its lower dimensional representation, anomalies can also be detected by analysing the reduced space [99]. There are several approaches that decompose data into normal, anomaly and noise subspaces such that anomalies lies within the anomaly subspace [38].

b: PRINCIPAL COMPONENT ANALYSIS (PCA)

PCA is a well-known linear dimensionality reduction technique that finds the directions of maximum variance in a dataset [93]. PCA can be used for AD by reconstructing data instances using only the first few principal components, and computing the reconstruction error. Anomalies can be detected by identifying data instances with high reconstruction error.

c: SUBSPACE-BASED METHODS

Subspace-based deviation methods involve decomposing the data into normal, anomaly, and noise subspaces based on their low-dimensional representation. Anomalies are assumed to lie within the anomaly subspace and can be identified as data instances that do not fit into the normal subspace.

d: LOW-RANK REPRESENTATION (LRR)

The LRR algorithm [94] uses a low-rank decomposition of the data matrix to obtain the normal and anomaly subspaces.

e: ROBUST-PCA

Robust-PCA [100] is a variant of PCA that is less sensitive to outliers in the data. In Robust-PCA, the data is decomposed into a low-rank matrix and a sparse matrix, such that anomalies are captured in the sparse matrix. The low-rank matrix captures the underlying structure of the data, while the sparse matrix is used to identify anomalies.

f: LIMITATIONS

One of the main limitations of deviation-based AD methods is that they require a careful choice of the feature space to capture the underlying patterns in the data. In addition, the performance of these methods can be sensitive to the choice of the decomposition technique and the number of dimensions used for the low-dimensional representation.

B. DEEP LEARNING-BASED ANOMALY DETECTION

This section presents deep learning-based AD techniques. Before the advent of deep learning, traditional AD methods relied heavily on handcrafted features. These methods have shown some success in detecting simple anomalies but often fail to detect complex anomalies [20]. Deep learning based AD has gained significant attention in recent years for its ability to learn complex patterns in data using neural networks. This has led to the development of various deep learning-based techniques for AD. This section provides a comprehensive overview of deep learning-based AD techniques. Table 1 summarises key previous work on deep learning-based AD. It highlights a significant focus on semi-supervised learning scenarios, particularly in the realm of image data because most of the advancements in this field have been driven by these applications. Section IV-B1 and IV-B2 present two principal approaches: solutions based on Autoencoders (AEs) and solutions leveraging Generative Adversarial Networks (GANs). The advancements in time series AD techniques that consider sequential data will specifically be presented in Section V.

TABLE 1. Summary of key previous work on deep learning-based AD. Symbols denote learning scenarios: ○ = unsupervised, ◉ = semi-supervised, ● = supervised. Among the algorithms examined, the majority were evaluated on image in semi-supervised learning scenarios.

Work	Year	Data Type	Scenario	Algorithms
[101]	2014	Spacecraft telemetry	◉	AE, DAE
[90]	2015	Images	◉	VAE
[102]	2017	Images	◉	RCAE
[103]	2017	Images	◉	DAE & RPCA
[104]	2017	Image markers	◉	DCGAN [105]
[106]	2018	Images	◉	GAN
[107]	2018	Images	○	AE & GMM
[108]	2018	Images	◉	BiGAN [109]
[110]	2018	Images	◉	OC-NN
[111]	2019	Images, TCP dump	◉	GAN
[112]	2019	Images	◉	WGAN [113]
[114]	2019	Images	◉	GAN
[115]	2019	Images	◉	AAE
[116]	2019	Images	◉	OC-NN
[117]	2021	Images, TCP dump	○	AE

1) AUTOENCODERS

AEs learn to encode and reconstruct input data. The original intention of using AEs is nonlinear dimensionality reduction and feature extraction [118]. Recent work however, suggests the use of deep AEs for AD [107], [115], [117]. AEs use the reconstruction error as the anomaly score. Typically, the AE is trained on normal data instances only in a semi-supervised fashion. During inference, the AE is able to reconstruct normal data accurately, while failing to reconstruct anomalous data that has not been observed during training. Data instances that result in high reconstruction errors are considered to be anomalous [90]. The sparse feature representation can also be extracted. This enables AEs to be useful in hybrid approaches in which the sparse feature representations obtained from the AE are processed by other AD algorithms [107], [117]. Methods suggested in previous work require the training data to be comprised of normal data instances only. However, data captured using monitoring sensors in real-world applications is subject to outliers and noise. To overcome this issue, previous work [102], [103], [117] suggests methodologies that are robust against corrupted data points. This subsection discusses various types of AE-based techniques, such as Denoising Autoencoders (DAEs) [101], [103], Convolutional Autoencoders (CAEs) [102], and Variational Autoencoders (VAEs) [90], Adversarial Autoencoders (AAEs) [115], and hybrid AE approaches [107], [117]. These AEs are designed to handle different types of data structures and address specific AD challenges.

a: VARIATIONAL AUTOENCODERS (VAES)

VAEs learn a generative model by combining the principles of AEs with those of Variational Inference [119]. The architecture of a VAE consists of an encoder and a decoder. The encoder maps the input data to a latent space, and the decoder generates the data from the latent space. VAEs work by learning a probabilistic representation of the data, and then using this representation to identify instances that deviate significantly from the learned distribution. The encoder and decoder are trained together [120]. An and Cho [90] proposed to use a VAE for AD and introduce the term *reconstruction probability* which is used as anomaly score. The encoder of the VAE is used to model the distribution of the latent variables and thus covers the variability of the latent space.

b: ADVERSARIAL AUTOENCODERS (AAES)

AAEs integrate the concepts of AEs with the adversarial training approach of GANs. Essentially, AAEs are neural networks trained to develop a probabilistic model of the dataset. The structure of an AAE includes an encoder, a decoder, and a discriminator. The encoder transforms the input data into a latent representation, the decoder generates the data from the latent space, and the discriminator tries to distinguish between the generated data and the real data. During the adversarial training process, the encoder, decoder, and discriminator are trained together. The encoder and decoder try to fool the discriminator by generating data that closely resembles the real dataset, while the discriminator tries to correctly identify the generated data [119]. Beggel et al. [115] adapted an AAE architecture in order to increase the performance of detecting anomalous images. The authors proposed a method called Iterative Training Set Refinement (ITSR) which is used to increase the robustness against contaminated datasets. Using a variation of a One-Class Support Vector Machine (OC-SVM), anomalous instances are identified and rejected during training, which results in a more robust anomaly detector. By imposing a prior distribution on the latent representation of the AE, anomalies are placed in the low likelihood region.

c: CONVOLUTIONAL AUTOENCODERS (CAES)

CAEs combine the principles of AEs with convolutional neural network layers. CAEs detect anomalies by learning hierarchical features in data, particularly in image and signal processing tasks. Chalapathy et al. [102] extended Robust-PCA [121] by proposing an AE model called Robust Convolutional Autoencoder (RCAE). This model learns a nonlinear subspace that captures the majority of data points while being robust against corrupted data points.

d: DENOISING AUTOENCODERS (DAES)

The primary difference between a DAE and a traditional AE lies in the training process. While traditional AEs aim to reconstruct the original input data, DAEs are trained to reconstruct the clean, noise-free version of the input data from its noisy counterpart. During the training process, noise is artificially added to the input data, and the DAE learns to recover the original, noise-free data from this corrupted version. By learning to remove noise and reconstruct the original data, DAEs become more robust to noise and can capture the essential features of the input data, improving their generalization capabilities. Sakurada and Yairi [101] used an AE and a DAE. Temporal dependency has not been considered because only a single multivariate point at a specific time step has been provided as input to the AE. Zhou and Paffenroth [103] proposed extensions that eliminate outliers and noise from the training data without prior knowledge. Their method called Robust Deep Autoencoder (RDA) is based on a combination of a DAE and Robust-PCA [121].

e: HYBRID AUTOENCODER APPROACHES

Hybrid approaches combine the strengths of multiple techniques to enhance detection performance and adaptability. These approaches involve using an AE to learn a sparse feature representation and compute the reconstruction error, which are then passed to another algorithm for the actual detection of anomalous data instances. The intuition behind hybrid approaches is to leverage the AE's ability to capture complex non-linear relationships in the data, while utilizing the strengths of other AD algorithms to effectively distinguish between normal and anomalous instances. Methods such as [107] and [117] combine the feature representation and reconstruction error process of an AE with another algorithm. In [122], the authors proposed the Deep Clustering Network (DCN) algorithm, that combines the representation learning process of an AE with K-means clustering. Zong et al. [107] adapted this concept by proposing their Deep Autoencoding Gaussian Mixture Model (DAGMM) method. Their method combines the dimension reduction process and reconstruction error of an AE with the density estimation process of a GMM. The parameters of the models are jointly optimized. In [117], the authors proposed a fully unsupervised iterative process that is based on an AE and clustering. Initially, the data instances are annotated through distribution clustering. Clusters with low variances are treated as normal, and these instances are used to train an AE. The class memberships of the compressed feature representations are then reevaluated based on distribution clustering. This process is repeated until the class membership of the data instances do not change anymore.

2) GENERATIVE ADVERSARIAL NETWORKS

GAN-based methods are popular deep learning-based AD techniques. GANs [123] are a type of neural network architecture that consists of two neural networks, a generator and a discriminator, that are trained together in a competitive way with the aim to generate realistic data samples. During inference, the generator produces fake data that is similar to the real data, while the discriminator tries to correctly identify the generated data. The generated data should be close enough to the real data, that the discriminator network cannot tell the difference. The GAN is typically trained using normal data to learn its underlying probability distribution. Anomalies are identified as the instances that have a low probability of being generated by the GAN. In the recent years, previous work proposed the Wasserstein GAN (WGAN) [113] and Cycle GAN [124] architectures that can potentially be used to replace the default GAN architecture. In the following we present various types of key GAN-based AD techniques, including AnoGAN [104], f-AnoGAN [112], GANomaly [106], Efficient GAN [108], Fence GAN [111], and Skip-GANomaly [114].

a: ANOGAN

Schlegl et al. [104] proposed AnoGAN, that is based on a Deep Convolutional Generative Adversarial Network (DCGAN) [125]. According to the authors, AnoGAN learns normal anatomical variability to assist radiologists in identifying disease markers in imaging data. The authors evaluated their experiments using a proprietary dataset that is comprised of Optical Coherence Tomography (OCT) images of the retina. Applications of the suggested method include diagnosis and monitoring of disease progression.

b: GANOMALY

Akcay et al. [106] introduced GANomaly, a GAN-based adversarial training framework that jointly learns to generate high-dimensional images, as well as the inference of latent space. An additional encoder network maps the generated images to its latent representations such that learning of the data distribution for the normal samples is emphasized.

c: EFFICIENT GAN

Zenati et al. [108] extended the Bidirectional Generative Adversarial Network (BiGAN) model proposed by Donahue et al. [109] to simultaneously learn an encoder, generator and discriminator during training without the need of recovering a latent representation at test time.

d: FENCE GAN

Ngo et al. [111] proposed Fence GAN. The authors modified the loss function of a GAN such that generated samples are distributed at the boundary of the real data distribution. This way the resulting discriminator is effectively tuned to the task of identifying anomalous images and the discriminator score directly serves as an anomaly threshold.

e: F-ANOGAN

Schlegl et al. [112] proposed f-AnoGAN to combine a GAN with a trained encoder that enables a fast mapping of images into the GAN's latent space to speed-up retinal OCT image AD. Their neural network architecture is based on a WGAN [113] in which the discriminator estimates the Wasserstein distance to differentiate between the real and the generator data distribution. The authors evaluated their experiments using a proprietary dataset that is comprised of OCT images of the retina.

f: SKIP-GANOMALY

The Skip-GANomaly architecture proposed in [114] is similar to GANomaly [106]. A major difference is that the authors introduced skip connections in the encoder-decoder convolutional neural network to capture the multi-scale distribution of the normal data.

V. ADVANCEMENTS IN TIME SERIES ANOMALY DETECTION

Time series AD deals with identifying unusual patterns in sequential data. Recent years have seen significant advancements in time series AD due to large-scale time series data and deep learning techniques. Deep learning-based methods, such as Recurrent Neural Networks (RNNs) [126], AEs [127], GANs [128], and Convolutional Neural Networks (CNNs) [129] have demonstrated success in addressing the challenges posed by time series AD tasks. These models can learn complex non-linear representations of the data, adapt to various types of anomalies, and provide better performance compared to traditional statistical and machine learning methods. This section covers various categories of deep neural networks used in time series AD, and their advantages and disadvantages. Table 2 lists recent literature on time series AD, summarizing each work based on the variate approach, the learning scenario, and the algorithms used.

In the field of time series AD, the choice of learning scenario often correlates with the specific application. This includes unsupervised approaches such as [126], [127], [128], [129], [132], [137], [139], and [140], semi-supervised approaches [130], [131], [133], [138], and supervised approaches [135], [136], [142]. Supervised learning, seen in [135], is prevalent in scenarios with well-defined anomalies, such as robot-assisted tasks, where labeled data is available. On the other hand, unsupervised learning, utilized in [137], is more suited to complex scenarios like spacecraft telemetry monitoring, where anomalies are not predefined and labeled data is scarce. Semi-supervised learning, as used in [130], strikes a balance, being useful in situations where normal data is known but anomalous data is not fully labeled.

Machine learning models, specifically RNNs and their variants, gained attention around 2016 [130], [131], [133], [137]. Malhotra et al. [130] detected anomalous sequences of unknown length using stacked Long Short Term Memory (LSTM) networks in a semi-supervised learning context for Electrocardiogram (ECG), space shuttle valve, power demand, and engine data. By assuming that prediction errors have a Gaussian distribution, the likelihood of anomalous behaviours was estimated. The use of LSTMs continued with studies like Malhotra et al. [131] in semi-supervised settings, and Bontemps et al. [133], Hundman et al. [137],

TABLE 2. Summary of previous works on time series AD. Symbols denote learning scenarios: ○ = unsupervised, ◉ = semi-supervised, ● = supervised. All algorithms examined are suitable for multivariate time series data with the tendency towards unsupervised learning scenarios.

Work	Year	Algorithms	Scenario	Time series	Area of Use	Datasets
[130]	2015	Stacked LSTM	◉	Multi	Various	ECG, Space shuttle, Power demand, Engine
[131]	2016	LSTM, Encoder-Decoder	◉	Multi	Various	ECG, Space shuttle, Power demand, Engine
[132]	2016	K-Means	○	Multi	Cow heat events	Proprietary (farm dataset)
[133]	2016	LSTM	◉	Multi	Network intrusion detection	KDDCup99 [134]
[135]	2017	CNN, HMM, MLP	●	Multi	Robot-assisted feeding hazards	Proprietary
[136]	2017	S-ESD, S-H-ESD	●	Multi	Cloud infrastructures	Proprietary
[137]	2018	LSTM	○	Multi	Spacecraft telemetry monitoring	SMAP [137], MSL [137]
[138]	2018	LSTM-VAE	◉	Multi	Robot-assisted feeding hazards	Proprietary
[139]	2018	ODCA	○	Multi	Various	Population, Climate, Satellite, Housing
[140]	2019	AE, S-RNN, Ensemble	○	Multi	Various	NAB [75], ECG
[127]	2019	GRU, VAE	○	Multi	Industrial device monitoring	SMAP [137], MSL [137], SMD [127]
[126]	2019	CNN, ConvLSTM	○	Multi	Various	Proprietary (synthetic data, power plant data)
[129]	2019	CNN	○	Multi	Various	Yahoo S5 [141], NAB [75]
[128]	2020	GAN	○	Multi	Various	MSL [137], SMAP [137], Yahoo S5 [141], NAB [75]
[142]	2020	Robust STL, CNN	●	Multi	Cloud and IoT monitoring	Yahoo S5 [141]

in unsupervised settings. In [131], Malhotra et al. proposed EncDec-AD, an encoder-decoder architecture based on LSTM networks. Temporal dependencies of the time series were captured by the LSTM network, and anomalies were detected by computing the reconstruction error. Bontemps et al. [133] used a LSTM to detect collective anomalies for network intrusion detection. The authors suggested to compute predictions errors that are above a threshold from multiple time steps to identify collective anomalies. Hundman et al. [137] proposed an unsupervised and non-parametric thresholding approach. Anomalies are identified by computing the residual of the predicted value and the true value for each variable in the time series separately. Their approach has been evaluated using expert-labeled telemetry anomaly data from the Mars Science Laboratory rover (MSL), Curiosity and the Soil Moisture Active Passive satellite (SMAP).

Novel machine learning models like VAEs, Gated Recurrent Units (GRUs), and GANs began to gain attention around the year 2017. Works like Park et al. [138], Su et al. [127], and Geiger et al. [128] reflect this trend. Park et al. [138] combined a LSTM with a VAE by replacing the feed-forward network of the VAE with a LSTM network. Using the architecture multiple signals are fused and their temporal dependencies are projected into the latent space of the encoder. The deviation between the expected distribution and the reconstructed distribution of the data is used to identify anomalies. Similarly, Su et al. [127] proposed OmniAnomaly, a stochastic RNN by making use of stochastic latent variables for robust data representations. A VAE maps the input data distribution into stochastic variables while GRUs model the temporal dependencies between these stochastic variables. Anomalies are detected by evaluating the reconstruction probability of an observation. The authors evaluated their method using the SMAP satellite [137] and MLS rover [137], and Server Machine Dataset (SMD) [127] datasets.

Geiger et al. [128] proposed to train an LSTM-based GAN model composed of an encoder, generator and discriminator. The encoder encodes the input sequence into a low-dimensional latent space, the generator tries reconstructing the input from the latent space, and the discriminator tries to classify it as either generated or real. To ensure that the generator reconstructs the input, they combine the Wasserstein loss function for GANs with the L2 reconstruction loss.

Ensemble methods also emerged, as seen in Kieu et al. [140], who used an ensemble of AEs, Sparsely-Connected RNNs (S-RNNs), and other models on the Numenta Anomaly Benchmark (NAB) [75] and ECG datasets. Kieu et al. [140] proposed and ensemble of AEs using S-RNNs which take a weight vector w_t to decide which hidden states should be used to compute the next hidden state. By using a different vector w_t for each network of the ensemble, this module learns a more diverse set of networks. They proposed two methods of ensembling. The first method uses independent networks where each encoder-decoder pair predicts an ouput on which the square error is calculated. In the second method they concatenate the hidden states of each encoder and use this concatenated hidden state as the input for a decoder.

Other methods proposed in previous literature for AD in time-series data leverage a variety of machine learning techniques and strategies. Shahriar et al. [132] tackled the problem with an unsupervised approach, focusing on three-dimensional accelerometer data from dairy cows. In their methodology, all individual time series were unified into a single time series, a strategy that closely resembles the approach by Lu et al. [139]. In the realm of robotics, Park et al. [135] used an anomaly classification network to detect faults in a feeding-assistant robot. Their solution involved computing temporal features from multi-modal sensor data with a Hidden Markov Model (HMM), and extracting convolutional features from camera images using the VGG16 CNN model [143]. Both, temporal and convolutional features were then fused by a Multi-Layer Perceptron (MLP), which used a softmax layer for the final anomaly classification.

Hochenbaum et al. [136] introduced Seasonal Extreme Studentized Deviate (S-ESD) and Seasonal Hybrid ESD (S-H-ESD) that decompose the time series into median, seasonality and residue in order to obtain the trend and seasonal components. Robust statistical metrics, such as the Median Absolute Deviation (MAD), were used to detect anomalies. Lu et al. [139] proposed an outlier detection algorithms that is based on Cross-correlation Analysis (ODCA). Multiple time series were simplified into a single time series by using the cross-correlation function. Zhang et al. [126] proposed their Multi-Scale Convolutional Recurrent Encoder-Decoder (MSCRED) method, which not only captures temporal dependencies and inter-correlations between time series but also provides robustness to noise. Their MSCRED constructs multi-scale signature matrices, uses a convolutional encoder and an attention-based Convolutional Long-Short Term Memory (ConvLSTM) network, and finally employs a convolutional decoder to reconstruct input signature matrices. Residual signature matrices are computed to detect anomalies. Munir et al. [129] introduced the DeepAnT algorithm that used a CNN for time-series forecasting, detecting anomalies based on the Euclidean distance between actual and predicted values.

The studies listed in Table 2 show that the majority of the studies dealt with multivariate data, indicating a trend towards tackling more complex and realistic datasets in the field. Furthermore, previous literature reveals an evolution of time series AD from using classical statistical methods towards complex machine learning models. It also highlights the continued use of unsupervised learning, indicating its importance in scenarios where labeled data are scarce or costly to obtain.

VI. COMMONLY USED DATASETS

A vital aspect of designing and evaluating AD algorithms is the availability of comprehensive and diverse datasets. This chapter briefly presents datasets that have been used in previous works, and Table 3 lists them thoroughly. An initial examination reveals several data types present in these datasets, including TCP dump [134], images (e.g., grayscale [144], [145], [146], color [147], [148], [149], [150], X-ray [106]), video frames [151], [152], and time series (e.g., space shuttle valve [153], power demand [154], NAB [75]). In terms of the number of instances, the KDDCup99 dataset [134] is the largest, with 494.021 instances. The KDDCup99 [134], MNIST [146], and CIFAR-10 [147] datasets have been heavily referenced in the literature [90], [102], [103], [106], [107], [108], [110], [111], [114], [115], [117], [133], [155], suggesting their prominent role in the research community. A closer look at the data reveals diverse dimensionality. Some datasets like Thyroid [134] and Arrhythmia [134] have fixed dimensions, i.e., 21 and 279 respectively. Others, have varying dimensionality, highlighting the diverse nature of data sources and capturing techniques. The tasks associated with the datasets span a wide range of applications. While KDDCup99 [134] focuses on intrusion detection, Thyroid [134] and Arrhythmia [134] lean towards disease detection. The Fashion-MNIST [144], USPS [145], and MNIST [146] are geared towards image, and digit recognition. Other tasks include crime detection [151], activity detection [152], and baggage threat detection [106]. The majority of the datasets are publicly available. However, the UBA [106] and FFOB [106] datasets remain private, due to the sensitive nature of their content. In the following, we briefly describe several of these datasets.

A. YAHOO! WEBSCOPE S5

The Yahoo! Webscope S5 dataset [141] is a benchmarking resource, especially for cloud computing infrastructures, where benchmark datasets are scarce. This dataset is segmented into four data classes (A1, A2, A3, and A4), were A1 contains real and A2-A4 contains synthetic web traffic metrics, tagged with anomalies. It consists of 371 files (67 real data, 304 synthetic data), where the real data has been human-labeled.

B. NAB

The Numenta Anomaly Benchmark (NAB) dataset [75] consists of over 60 real-world and artificial univariate time series data files. The real-world data includes Amazon server metrics like CPU utilization, online advertisement clicking rates, data with identified anomaly causes, covering areas from office temperatures to industrial machinery failures, traffic information from Minnesota's Twin Cities Metro area, as well as Twitter mentions of major publicly-traded companies.

C. UCR ARCHIVE

The UCR Time Series Data Mining Archive [162] is a comprehensive collection of over 100 time series datasets. Among others, the archive includes the Electrocardiograms (ECG200), space shuttle, and power demand datasets.

D. ECG200

The ECG200 dataset is pivotal for heart health research as it captures the electrical activity recorded during a single heartbeat. Normal heartbeat and a heart attack are distinguished.

E. SPACE SHUTTLE

Space Shuttle dataset [153] consists of solenoid current measurements of a Marotta MPV-41 series valve, a critical component for fuel flow regulation in a space shuttle. This dataset, generously donated by NASA's Kennedy Space Center, is instrumental in identifying and understanding potential anomalies in aerospace missions.

TABLE 3. Datasets previous work commonly used for the development and evaluation of AD algorithms. The datasets cover a wide array of application areas such as network intrusion detection, disease detection, image and digit recognition, crime detection, and more, indicating the breadth of AD applications in different fields.

Work	Dataset	Dimensionality	Data type	Area of Use	Instances	Public	Labels	References
[134]	KDDCup99	1 × 120	TCP dump	Network intrusion detection	494021	Yes	Yes	[90], [107], [108], [111], [117], [133]
[134]	Thyroid	21	Numeric, Categorical	Disease detection	7200	Yes	Yes	[107]
[134]	Arrhythmia	279	Numeric	Arrhythmia classification	452	Yes	Yes	[107]
[144]	Fashion-MNIST	28 × 28	Grayscale images	Image classification	70000	Yes	Yes	[115]
[145]	USPS	16 × 16	Grayscale images	Digit recognition	9298	Yes	Yes	[102]
[146]	MNIST	28 × 28	Grayscale images	Digit recognition	70000	Yes	Yes	[90], [103], [106], [108], [110], [111], [115], [117], [155]
[147]	CIFAR-10	32 × 32	Color images	Image classification	60000	Yes	Yes	[102], [106], [110], [111], [114], [117], [155]
[148]	CatVsDog	128 × 128	Color images	Human interactive proof	15000	Yes	Yes	[117]
[151]	UCF-Crime	Varying	Surveillance videos	Crime detection	Varying	Yes	Yes	[117]
[152]	Restaurant	120 × 160	Video frames	Activity detection	500 [156]	N/A	N/A	[102]
[106]	UBA	N/A	X-ray images	Baggage threat detection	230275 [157]	No	N/A	[104], [114]
[106]	FFOB	N/A	X-ray images	Baggage threat detection	72352 [157]	No	N/A	[104], [114]
[158]	1001 Abnormal Objects	Varying	Color images	Object classification	1001	Yes	Yes	[116], [159]
[160]	UMDAA-02	Varying	Smartphone sensor signals	User authentication	Varying	No (Full) / Yes (Face)	Yes	[116], [159]
[149]	Caltech-256	Varying	Color images	Image classification	30607	Yes	Yes	[116]
[150]	GTSRB	Varying	Color images	Traffic sign recognition	51839	Yes	Yes	[110]
	ECG200	1	Electrocardiogram time series	Heart attack detection	200	Yes	Yes	[130], [131]
[153]	Space Shuttle Marotta	1	Space Shuttle valve time series	Space Shuttle fuel flow	15000 [131]	Yes	Partial	[130], [131]
[154]	Dutch power demand (DPD)	1	Power demand time series	Power demand AD	35040	Yes	No	[130], [131]
	Engine	12	Sensor readings	Engine fault detection	N/A	No	N/A	[130], [131]
[75]	NAB	1	Time series data	Varying	Varying	Yes	Yes	[128], [129], [140]
[141]	Yahoo! Webscope S5	2 (timestamp, value)	Numeric (real, synthetic)	AD benchmarking	Varying	Yes	Yes	[161]

F. POWER DEMAND

The power demand dataset [154] consists of a year's worth power consumption measurements collected at a Dutch research facility. Such data is invaluable for energy management and efficiency studies.

G. ENGINE

The Engine dataset is sourced from a real-life industry project and encompasses readings from 12 different sensors related to an engine. The dataset is utilized to train detectors using sequences corresponding to three independent engine faults. Due to its industry-specific nature, this dataset is not publicly available.

H. KDDCUP99

The KDDCup99 dataset [134] has been created by MIT Lincoln Labs in 1998. The dataset consists of one-hot encoded TCP network traffic data that was collected over a period of 5 weeks. It is intended for the development of network intrusion detection algorithms. A variety of intrusions have been simulated in a military network environment. The "normal" samples in the dataset are the minorities, for this reason they are treated as anomalies.

I. THYROID

The Thyroid dataset [134] is obtained from the UCI machine learning repository. The Thyroid dataset, comprises 3772 training and 3428 testing instances, with 15 categorical and 6 real attributes. The dataset contains three classes representing different thyroid conditions. The hyperfunction condition, being the least common, is treated as an anomaly. The remaining two classes serve as a contrast. Commonly, 3772 training instances, with 6 real attributes are used.

J. ARRHYTHMIA

The Arrhythmia dataset [134] is obtained from the UCI machine learning repository. The dataset is designed to distinguish between the presence and absence of cardiac arrhythmia. Featuring 274 attributes, this set comprises data on aspects like age, sex, height, weight, heart rate, and various ECG measurements. The smallest classes (3, 4, 5, 7, 8, 9, 14, and 15) are merged to form an anomaly class, while the rest make up the normal class.

K. USPS

The USPS dataset [145] consists of gray-scale digit images taken from envelopes scanned by the U.S. Postal Service.

L. MNIST

The MNIST dataset [146] has a training set of 60000 images, and a test set of 10000 images. The gray-scale images have a resolution of 28 × 28 pixels and show handwritten digits from 0 to 9.

M. FASHION-MNIST

The Fashion-MNIST dataset [144] has very similar properties compared to the MNIST dataset. The images size and proportion of training and testing images are the same. The images show clothing article from the Zalando's web shop instead of handwritten digits. Each image is annotated with a label from 10 article classes.

N. CIFAR-10

The CIFAR-10 dataset [147] consists of 60000 color images, divided into 50000 training images and 10000 test images. Each image has a size of 32×32 pixels and is annotated with a label from one of 10 object classes.

O. UCF-CRIME

The UCF-Crime dataset [151] comprises 1900 surveillance videos captured from CCTV cameras. The dataset is large-scale with a total video length of 128 hours. Each video is annotated with a label from 13 different categories of real-world crimes (e.g. abuse, burglary, shooting). The categories have been selected because they impact public safety. The UCF-Crime dataset has been specifically created for development and evaluation of AD algorithms.

P. UBA

The University Baggage Anomaly (UBA) dataset [106] is derived from X-ray images. The abnormal classes include 3 sub-classes, namely knife, gun, and gun component.

Q. ASIRRA

The Animal Species Image Recognition for Restricting Access (ASIRRA) dataset [148] comprises images taken from cats and dogs. The dataset has been specifically designed to protect access to web services via the use of CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart).

R. CATVSDOG

The CatVsDog dataset has been extracted from the ASIRRA dataset [148]. It comprises 12500 color images of dogs and 2500 images of cats that have a resolution of 128 × 128 pixels. Since the cat images are the minorities, they are treated as anomalies.

As shown in Table 3, it is evident that these datasets are predominantly public and labeled, facilitating their use in both academic and industrial research. The fields covered by these datasets range from network intrusion and disease detection to image classification and crime detection, highlighting the widespread applicability and importance of AD across different sectors.

VII. ANOMALY DETECTION IN SMART ENVIRONMENTS

This section reviews recent literature on AD in a variety of smart environments including, smart home, smart transport, and smart industry as visualized in Figure 15. The methodology employed in this survey is detailed below to clarify the scope and rigor of the research process.

Period Considered: Recent literature in this context specifically refers to a period covering the last five years, from 2019 to the present. The focus on this timeframe was chosen to ensure that the analysis remains relevant to current technological advancements and trends in AD.

Database and Queries: The research employed the Digital Bibliography & Library Project (DBLP) [163] as the primary database, we also utilized Google Search and Scopus. Queries were specifically tailored to each domain, namely ‘smart home anomaly detection’, ‘smart transport anomaly detection’, and ‘smart industry anomaly detection’. This targeted approach ensured a focused retrieval of relevant literature.

Filtering Criteria: To maintain a high standard of academic rigor, the selection of papers was filtered based on two criteria. Firstly, the h5-index of the publisher was assessed using Google Scholar [164]. Papers published by sources with an h5-index of 15 or higher were considered. Secondly, for conference papers, a threshold of 15 or more citations was set as an inclusion criterion. This dual-filter approach ensured that well-regarded and influential papers were reviewed. We have also considered works that go beyond these criteria if they represent innovative steps in the field.

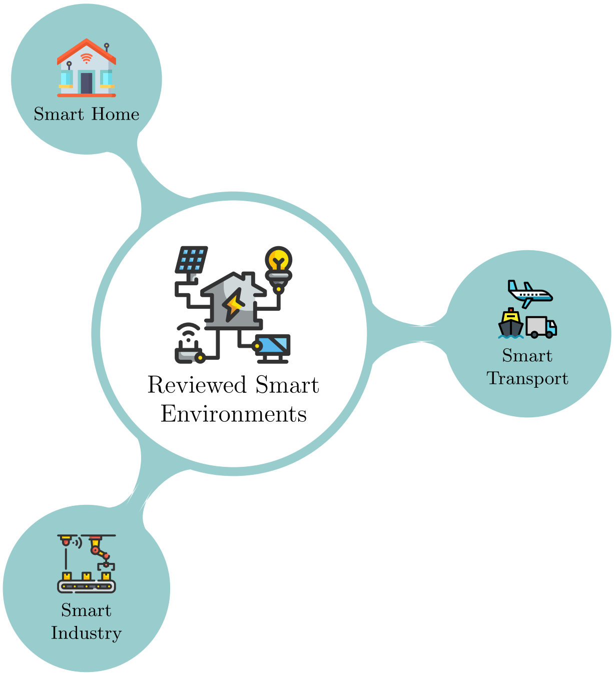


FIGURE 15. This figure presents a visual summary of the key smart environments explored in this survey, specifically focusing on AD applications in smart home, smart transport, and smart industry sectors.

A. SMART HOME

In recent years, the integration of smart technologies into homes, has been identified as a critical tool in enhancing the quality of life of individuals, particularly among the elderly population. Central to this advancement is the objective to enrich the life experiences of inhabitants through the incorporation of human-centered applications [165]. Health Smart Home (HSH) refers to a smart home that has an integrated health monitoring system [43]. HSHs aim at reducing the needs for healthcare services, so that elderly individuals can live independently for a longer time. HSHs also aim at reducing costs and the workload on the overall health system [42], [43]. In previous work, technological approaches in facilitating activity recognition and pinpointing behavioral deviations were proposed. These are critical components in augmenting healthcare provision for elderly individuals [165]. According to [166], the current demographic shift towards an aging population necessitates a strong focus on home care systems. These structures are becoming pivotal in addressing the rising need for elderly care, with Ambient Assisted Living (AAL) environments at the helm of this revolution.

1) USE CASE SCENARIOS

In the rapidly evolving landscape of smart homes, a diverse range of techniques have been employed to address various use cases. According to [167], these use cases can be categorized into: a) temporal (duration), b) temporal (time of occurerence), c) spacial, d) pattern of action, e) environment changes and f) context switching use cases. Due to the demographic shift towards an aging population, home care systems are becoming increasingly important. According to [166], applications in home care systems predominantly span across: a) emergency assistance, b) autonomy enhancement, and c) comfort services. Figure 16 visualizes a comprehensive overview of the various use cases investigated in previous research. These use cases span across multiple application areas, each addressing unique challenges within smart transport environments. In the following, the application areas and the particular use cases are described in detail:

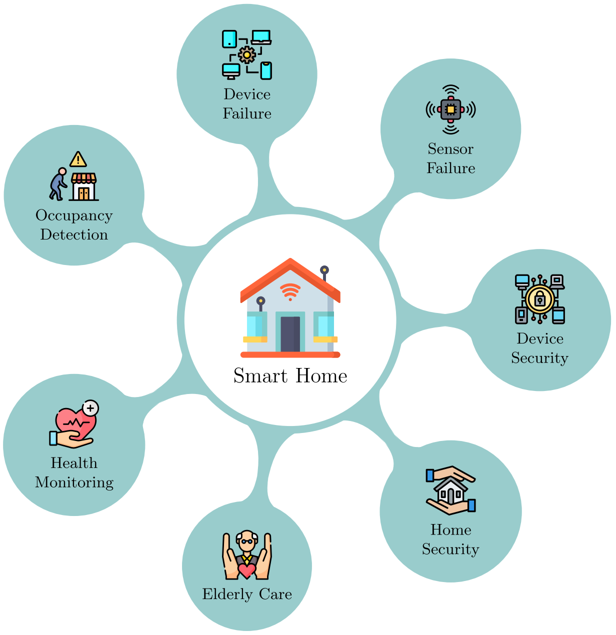


FIGURE 16. **Use cases for AD in smart homes.**

a: ELDERLY CARE

This category encompasses applications designed to enhance the safety and well-being of the elderly. It includes research on fall detection [66], [168], [169], recognition of daily activities [170], and elderly monitoring systems [171].

b: HEALTH MONITORING

This category addresses the monitoring of health and behavioral patterns, including detection of deviations in patient behavior [165], [172], identification of clinically significant health events [173], health problem detection [174], and monitoring activities of daily living for health assessment [175].

c: HOME SECURITY

This category encompasses works that focus on home security (e.g., unauthorized access, potential hazards) [176], cybersecurity (based on energy consumption) [177], network cyberattack detection [178], and ensuring trust and integrity [179].

d: DEVICE SECURITY

This category includes previous work on IoT attack detection [180] and analyzing IoT network traffic for security purposes [181].

e: SENSOR OPERATIONAL MONITORING

Previous work in this category is focused on the detection and diagnosis of sensor failures [182], [183] and the identification of sensor data corruption [184].

f: DEVICE OPERATIONAL MONITORING

This category encompasses research on device malfunction detection [185], and operational analysis of smart home IoT devices [186].

g: OCCUPANCY DETECTION

Previous work on occupancy detection includes [66], [187], [188].

2) TYPICAL SENSORS

The section elaborates on several types of sensors and their respective utilities based on previous work.

Electric sensors such as smart meters, have been employed for cybersecurity [177] and ensuring trust and integrity [179]. Light sensors are used for health monitoring in smart homes [172] and occupancy detection [66], [187], [188]. Infrared sensors are used for the detection of clinically meaningful health events [173]. Electromagnetic sensors such as WiFi-based systems, are used in network cyberattack detection [178], and IoT network traffic analysis [181]. Wearable localization tags are utilized in fall detection applications [66], [168], [169]. Temperature sensors are used for health monitoring [172], occupancy detection [66], [187], [188], and elderly monitoring [171]. Motion sensors are used for sensor failure detection [170], [171], [175], [182], [183], [185]. Magnetic door sensors are employed in the detection of clinically meaningful health events [173]. Door closure sensors are used for elderly monitoring [171]. Fusion sensors, like the Zooz 4-in-1 sensor, are utilized for the detection of device malfunctions [185]. Weather station sensors are used for the detection of sensor anomalies [184]. CO2 sensors are utilized in occupancy detection [66], [188].

3) LITERATURE REVIEW

This section presents a literature review on AD in smart homes. Table 4 provides a comprehensive overview, showcasing a variety of approaches and applications over the years. The algorithms used, the learning scenarios, the applications, the sensors employed, and the datasets used for evaluation are listed.

The learning scenario often correlates with the application, including supervised approaches [66], [168], [169],

TABLE 4. Summary of previous work on AD in smart home environments. Symbols denote learning scenarios: ○ = unsupervised, ⦿ = semi-supervised, ● = supervised. Additional symbols for anomaly types: ⊡ = point anomalies, ⊟ = context anomalies, ⊠ = collective anomalies. The most noticeable aspect is the predominance of supervised learning approaches (●), indicating a strong reliance on labeled data for model training. Another standout observation is the diversity of applications covered. Lastly, the evolution from simpler to more complex algorithms, such as the use of DNNs and ensemble models, highlights the field's technological advancements over time.

Work	Year	Algorithms	Scenario	Area of Use	Sensors	Anomaly Type	Dataset
[182]	2014	FailureSense (GMM)	⦿	Sensor failure detection	Motion	⊡, ⊟, ⊠	Houses [189]
[168]	2014	CDKML (NaiveBayes, RF, SMO, JRip, J48)	●	Fall detection for elderly	Wearable Localization Tags	⊡, ⊟	Fall detection [190]
[165]	2015	Sequence Mining, Extended Finite Automaton (EFA)	○	Health monitoring, behavioural deviations of patients	Various	⊟, ⊠	Domus Smart Home Dataset
[169]	2015	Confidence System	●	Fall detection for elderly	Wearable Localization Tags, Accelerometers	⊡, ⊟, ⊠	Fall Detection [190]
[172]	2016	BCD (sw-PCAR, VC)	●	Health monitoring, behavioural deviations of patients	Motion/Light, Door/Temperature	⊟	CASAS [191]
[187]	2016	RF, LDA, CART, GBM	●	Occupancy detection	Light, Temperature, Humidity, CO2	⊡, ⊟, ⊠	UCI Occupancy Detection [187]
[192]	2018	MCRN	●	Various	Various	⊡, ⊟, ⊠	Multiple UCI datasets [134]
[176]	2019	HMM	●	Home security (unauthorized access, potential hazards)	Various IoT Devices	⊟, ⊠	Not specified
[188]	2019	MVCNN	●	PHM challenge, occupancy detection	Light, Temperature, Humidity, CO2	⊡, ⊟, ⊠	PHM 2015, UCI Occupancy Detection [187]
[193]	2019	Ensemble Model, Decision Tree, Gaussian Naive Bayes, Logistic Regression	●	Smart home IoT devices	Motion, Power, Temperature	⊟, ⊠	CASAS [191]
[186]	2020	User behavior modeling	⦿	Smart home IoT device operation	Home IoT Devices	⊡, ⊟	Proprietary
[184]	2020	AE	○	Sensor anomalies	Weather Station	⊡	Proprietary
[185]	2021	HAWatcher	⦿	Device malfunctions	Various (Motion, Illuminance, Humidity, Switches, etc.)	⊡, ⊟	Proprietary
[177]	2021	Kalman Filter, Shapiro-Wilk Test	○	Cybersecurity (based on energy consumption)	Smart Meters	⊡	Simulated MATLAB Scenarios
[174]	2021	Model-Based Approach	⦿	Health problems	Not Specified	⊡, ⊟	DOMUS
[173]	2021	Isudra, Bayesian Optimization	⦿	Clinically meaningful health event detection	PIR Motion, Magnetic Door	⊡, ⊟	CASAS [191]
[170]	2021	PNN, H2O Autoencoder	⦿	Elderly daily activity recognition	Motion, Contact Switch, Item Status, Door	⊡, ⊟	Aruba, Milan (CASAS) [191]
[183]	2022	DNN, HSC	●	Sensor failure detection	Binary (Motion, Door)	⊡	Aruba (CASAS) [191]
[178]	2022	Logistic Regression, Naïve Bayes, Decision Tree, K-NN, SVM, RF, XGBoost	⦿	Network cyberattack detection	Network Traffic Data	⊡	Simulated Smart Home Test-Bed Data
[179]	2022	ARIMA, SARIMA, LSTM, Prophet, Light GBM, VAR	○	Trust and integrity	Smart Meter, Weather	⊡	Smart Home Dataset with Weather Information
[171]	2022	DNN, OCD-AE, LSTM	⦿	Elderly monitoring	Motion, Door Closure, Temperature	⊡, ⊟	Aruba, Cairo
[66]	2022	DDQN with PER	●	Fall and occupancy detection	Light, Temperature, Humidity, CO2, Wearable Localization Tags	⊡, ⊟, ⊠	Fall Detection [190], UCI Occupancy Detection [187]
[175]	2023	Multivariate LSTM, Mahalanobis Distance	○	Detection of ADLs	Motion	⊟	Proprietary
[180]	2023	AE, k-means	○	IoT attack detection	IPFIX Metadata	⊡, ⊟, ⊠	CADeSH [194]
[181]	2023	AdaBoost, Decision Trees, RF, LSTM-AE, ANN	●	IoT network traffic analysis	Network traffic features	⊡, ⊟, ⊠	UNSW BoT IoT

[172], [181], [183], [186], [187], [188], semi-supervised approaches [165], [170], [171], [173], [174], [175], [178], [182], [185], and unsupervised approaches [177], [179], [180], [184], [192], [193], [195]. Supervised learning, seen in [168], is common in well-defined scenarios like fall detection, while unsupervised learning, as used in sensor AD [184], suits more complex scenarios.

Approaches for health monitoring and elderly care have been proposed in previous work, with advanced systems like multi-agent models and deep learning techniques to detect falls and monitor daily activities [168], [169], [170], [171], [172], [173], [195]. Mirchevska et al. [168] developed a method named Combining Domain Knowledge and Machine Learning (CDKML). This method uses domain knowledge enriched with machine learning patterns, refined through genetic algorithms, and adapted online using user feedback. It involves three phases, namely: initialization, refinement, and online adaptation. Initially, a classifier is developed using traditional rule-based and decision tree algorithms, which is then refined using genetic algorithms under expert supervision. Finally, an online learning process adapts the classifier based on user feedback. In [169], the authors enhanced their confidence system, initially introduced in [195], by incorporating additional accelerators to improve the fall detection accuracy. Sprint et al. [172] developed the Behavior Change Detection (BCD) approach to discern behavioral changes and their possible correlations to health alterations. Utilizing machine learning techniques, including small-window PCAR (swPCAR) and Virtual Classifier (VC) methods, they demonstrated the feasibility of monitoring significant health-related behavioral changes. Dahmen and Cook [173] introduced Isudra, an indirectly supervised AD system for smart homes, using Bayesian optimization, focusing on health-related anomalies like falls and depression. Fahad and Tahir [170] introduced an approach combining Probabilistic Neural Network (PNN) and H2O autoencoder for elderly daily activity recognition. Alaghbari et al. [171] developed a unified deep learning model for elderly monitoring, integrating activity recognition via Deep Neural Network (DNN), AD with Overcomplete-Deep Autoencoder (OCD-AE), and next activity prediction using LSTM. This comprehensive approach, tested on Aruba and Cairo datasets, aims to assist caregivers in understanding and responding to elderly residents needs and behaviors.

Another focus of the research was on the detection of behavioral deviations in medically monitored patients [165], [174], [175]. Saives et al. [165] concentrated on detecting behavioral deviations among medically monitored patients. Utilizing sequence mining techniques, they synthesized daily activities of the inhabitants to construct a recognition model capable of detecting both short-term and long-term deviations in the patients' habits, thereby offering an insightful approach to patient monitoring. Fouquet, Faraut, and Lesage [174] developed a model-based approach for AD in the daily lives of smart home inhabitants. Employing activity ordering and duration analysis, the method aims to identify behavioral deviations indicative of health issues, using the publicly available DOMUS database for validation. In [175], the authors utilized a Multivariate LSTM model and Mahalanobis distance for unsupervised forecasting and AD of Activities of Daily Living (ADLs) in elderly smart homes. Their research, based on motion sensor data, aims to detect changes in health conditions and support independent living for the elderly.

Approaches for the detection of room occupancy have been proposed [66], [187], [188], [196]. In [187], the authors presented several models to tackle the occupancy detection problem. The evaluated models include Random Forest (RF), Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART), and Gradient Boosted Models (GBM). The performance of these models varied, with accuracies ranging from 93.06% to 98.76% on the proposed

UCI Occupancy Detection dataset. Liu et al. [188] proposed a novel deep learning architecture called Multivariate Convolutional Neural Network (MVCNN). Their MVCNN was evaluated using both, the PHM 2015 challenge dataset and the UCI Occupancy Detection dataset. In [66], the authors proposed an adaption of the Double Deep Q-Learning (DDQN) algorithm, traditionally rooted in deep reinforcement learning. By extending DDQN with a Prioritized Experience Replay (PER) strategy, the algorithm enables rare event classification and showed promising results in occupancy and fall detection applications.

Other work focused on methods for sensor and device operational monitoring, such as the detection of sensor failures [182], [183], device malfunctions [185], and the operation of IoT devices [186]. Munir and Stankovic [182] introduced FailureSense, an approach for detecting sensor failures. Utilizing data from electrical appliances, FailureSense aims at identifying various sensor failures, including fail-stop, obstructed-view, and moved-location failures. The method involves learning the typical patterns of sensor activity in relation to appliance use and detecting deviations from these patterns as indicators of sensor failure. Jung et al. [183] developed a DNN-based method for detecting simultaneous sporadic sensor anomalies in smart homes, utilizing Hypersphere Classification (HSC). Evaluated on the Aruba dataset, their method demonstrated robustness, especially in scenarios with multiple faulty sensors. Fu et al. [185] introduced HAWatcher, a semantics-assisted system for smart homes, leveraging smart app semantics and event log data. Their method detects discrepancies between expected and observed behaviors in IoT environments, achieving high accuracy in four real-world SmartThings testbeds. Yamauchi et al. [186] proposed a method for smart home IoT devices based on learning user behavior patterns and home conditions. Their method successfully detects anomalous operations, emphasizing the importance of learning event sequences and user habits.

Another major application area is focused on Home and IoT devices security [176], [177], [178], [179], [180], [181], [184]. In [176], the authors developed an HMM-based model for identifying simulated attack scenarios. This model effectively learned and identified typical behaviors, setting a groundwork for future enhancements in smart home security. In [184] the authors demonstrated the use of a convolutional AE for detecting anomalies in smart home sensors. Their study emphasizes early detection of data corruption in smart grid systems, using a proprietary dataset from weather station sensors. Alsabilah and Rawat [177] proposed a cybersecurity monitoring system for smart homes using the Kalman Filter and Shapiro-Wilk test. Focusing on energy consumption data from smart meters, their method detects cyber-attacks and abnormal device behaviors in smart home networks. Priyadarshini et al. [179] conducted a study on time series analysis, employing AutoRegressive Integrated Moving Average (ARIMA), Seasonal ARIMA (SARIMA), LSTM, Prophet, Light GBM, and VAR algorithms. Focusing on energy consumption and weather data, the research utilized the Sequentially Discounting AutoRegressive (SDAR) based Change Finder algorithm, demonstrating that the ARIMA model outperformed others in terms of accuracy. Li et al. [178] developed a method for improving network-based AD, utilizing traditional and ensemble machine learning classification methods. Their approach, which included simulating network attacks, detected anomalies in IoT device behavior. In [181], Sarwar et al. apply various algorithms to IoT network traffic analysis using the UNSW BoT IoT dataset, aiming to improve security monitoring in smart environments. Meidan et al. [180] proposed CADeSH, a collaborative AD method using AEs and k-means clustering. Focusing on IoT device network traffic, the research leverages a novel, publicly available dataset from multiple home networks.

4) DATASETS

This section presents various datasets that have contributed to the development of AD algorithms in smart home environments. Table 5 presents an overview of these datasets, including information such as the nature of the data (whether public or otherwise), the labels associated with the data, the dimensionality, and the number of instances.

a: UCI OCCUPANCY DETECTION

The UCI Occupancy Detection dataset [187], encompasses real-world sensory data that can facilitate the creation of methods to accurately determine room occupancy. This dataset comprises readings from various sensors monitoring aspects such as light, temperature, CO2 levels, and humidity, alongside timestamps and humidity ratios. These factors are pertinent as many modern smart buildings are already equipped with these sensors. The dataset is divided into a training and two testing series. Notably, the ground truth labels in the dataset were acquired automatically through a video surveillance system.

b: KASTEREN UBICOMP

The Kasteren Ubicomp dataset [197] was developed for activity recognition using ambient sensor readings instead of typical wearable sensors. Recorded in a multi-room apartment with one resident, it features 1319 sensor intervals from 14 digital state-change sensors and 245 manually annotated activity intervals using a Bluetooth headset for verbal annotations. The data was captured over 28 days, from 25.02.2008 to 23.03.2008.

c: HARVARD OCCUPANCY DETECTION

The Harvard Occupancy Detection Dataset (ODD) [198] offers a comprehensive collection of sensor readings related to power consumption, ambient conditions, and weather patterns. The dataset encompasses readings from power meters, ambient light sensors, and ambient temperature sensors. Furthermore, it integrates local weather conditions

TABLE 5. Smart home dataset overview with general information. A significant aspect is the accessibility of these datasets, with most being publicly available and often labeled, indicating a trend in the field of smart home AD. Among the datasets listed, the "MavPad" is the largest in terms of instances.

Work	Dataset	Dimensionality	Instances	Public	Labels	Environment
[187]	UCI Occupancy Detection	7	20560	Yes	Yes	Office room
[197]	Kasteren Ubicomp	6	1319	Yes	Yes	Home environment
[191]	CASAS	Various	Various	Yes	Partial	Home environments
[198]	Harvard ODDs	Various	Various	Yes	Partial	Home environment
[199]	MavPad	7	4371130	Yes	No	Student apartment
[199]	MavLab	4	4208	Yes	No	Office environment
[190]	Fall detection	4	164259	Yes	Yes	Home environment

and daily sunrise and sunset data, providing a holistic view of the environment over a span of approximately 8 months.

d: CASAS

The CASAS dataset [191] is a comprehensive collection of smart home data accumulated through various testbeds, primarily focusing on monitoring activities of daily living. It encompasses data from different geographic locations named like Kyoto, Tulum, Tokyo, and others, featuring varied environments ranging from single-resident apartments to multi-resident homes, and even some inclusive of pets. A significant portion of this dataset is formed by the inclusion of data from 30 distinct apartments labeled HH101 to HH130. These apartments, were equipped with smart ambient sensors, installed by volunteer residents. While most of these apartments are unique in structure, a few of them share similar layouts. The datasets gathered from these apartments primarily involve single-resident environments, with the exception of HH107 and HH121, which house two residents each. The sensor setup in each apartment varies, accommodating the distinct layouts by altering the number and placement of sensors, although the type of sensors remains consistent across the board, including light, motion, magnetic, and temperature sensors. These dataset provides partial annotations.

e: MAVLAB

The MavLab dataset [199] offers insights into sensor events recorded in the MavLab testbed, an automated office environment located in the Engineering Building at the University of Texas at Arlington (UTA). Spanning the months of March and April in 2003, the data encompasses the daily routines of approximately six students who worked there regularly. MavLab's design mirrors a standard office, complete with cubicles, a lounge, a kitchen, a dining space, and a meeting room. It's automation is made possible with 54 X-10 controllers. The facility is fitted with an array of sensors that detect light, temperature, motion, humidity, and the status of doors and seats. Furthermore, the lab can regulate lights, appliances, fans, heaters, and window blinds.

f: MAVPAD

The MavPad dataset [199] provides a comprehensive view of sensor events from the MavPad testbed, an on-campus student apartment situated in University Village at The University of Texas at Arlington. This apartment features a combined living and dining area, kitchen, bathroom, bedroom, and a walk-in closet. The range of sensors deployed within this environment is extensive, encompassing motion, light, temperature, humidity, reed switch, smoke, and gas detectors. The data presented in this dataset were accumulated throughout 2005 when the apartment was home to a single resident.

g: FALL DETECTION

The Fall Detection dataset developed by Kaluza et al. [190] is a comprehensive collection of local position data gathered with the purpose of advancing activity recognition and healthcare for the elderly, ultimately aiming to enhance the safety of seniors living independently. It utilizes the Ubisense localization system, featuring four distinct accelerometers positioned at various body points: the chest, belt, and both the left and right ankles. It encompasses a total of 164259 samples, divided into 134229 training and 30030 testing samples, further segmented into 25 separate parts, with a specific allocation of 20 parts exclusively for training and the remaining 5 parts dedicated to testing procedures. Notably, the sensor readings within this dataset demonstrate high volatility, which is captured and wirelessly transmitted in real-world settings. This data consists of a relatively small percentage of anomalous samples. Specifically, the training set contains 4.9% anomalous samples, whereas the testing set comprises 5.4%.

Among the datasets presented in Table 5, a notable trend is the availability of public data, essential for developing and validating smart home AD algorithms [191], [197], [198], [199]. However, there is a notable lack of datasets that comprehensively cover multi-resident environments, as most datasets focus on single-resident settings or specific aspects of smart home environments, such as occupancy [187] or fall detection [190]. This gap highlights a potential area for future dataset development to better address the complexities of multi-resident AD scenarios in smart homes.

B. SMART TRANSPORT

Smart transport environments capture data to analyze traffic patterns in transportation networks. The traffic data originating from vehicles such as cars, trucks, or bicycles can be used to detect and classify different types of anomalies. These anomalies could lead to potential safety issues if not detected at an early stage [201].

1) USE CASE SCENARIOS

Smart transport systems are increasingly utilizing AD applications to enhance urban mobility and safety. Figure 17 visualizes a comprehensive overview of the various use cases investigated in previous research. In the following, the application areas and the particular use cases are described in further detail:

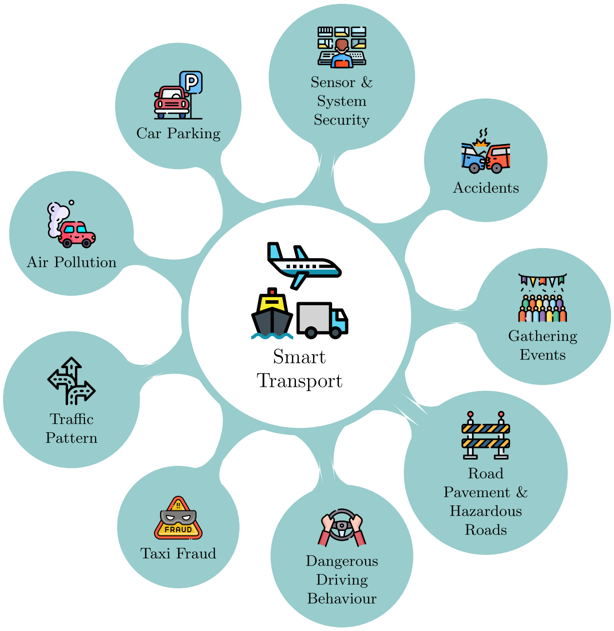


FIGURE 17. Use cases for AD in smart transport.

a: TRAFFIC PATTERN ANALYSIS

This category involves detecting anomalous traffic patterns. It includes traffic pattern analysis [202], root cause analysis of traffic anomalies [203], traffic anomalies detection [204], and unusual traffic flow detection [205], [206], [207].

b: TAXI AND DRIVING FRAUD DETECTION

This category focuses on identifying fraudulent activities in taxi services and driving behaviors. It includes taxi driving fraud detection [208], [209], [210], [211], anomalous taxi trip detection [212], dangerous driving behavior detection [161], and road pavement analysis [213].

c: EVENT AND GATHERING DETECTION

This category covers the identification of significant events and gatherings. It includes gathering event detection [59], [61], [88], [214], and unusual event detection like concerts or accidents [63], [215].

d: TRANSPORTATION SYSTEM SECURITY

This category addresses security aspects, including data integrity and sensor security in transportation systems. It encompasses data integrity attacks [216], automotive sensor security [217], sensor faults and failures [218], and intelligent transportation system security [219].

e: ENVIRONMENTAL MONITORING AND PUBLIC HEALTH

This category includes studies on environmental factors and public health, such as air pollution analysis [220], traffic accident risk assessment [221], and traffic incident detection [222]

f: ANOMALOUS TRAJECTORY AND LOCATION DETECTION

This category focuses on identifying unusual trajectories and locations, including anomalous trajectories on road segments [223], anomalous trajectories detection [224], and parking location anomalies [225], [226].

g: VARIOUS URBAN ANOMALIES

This category includes the detection of various urban anomalies [226], including noise issues, blocked driveways, illegal conversions of residential buildings, and illegal parking.

2) TYPICAL SENSORS

This section presents sensors commonly utilized for AD in smart transport environments.

GPS sensors are extensively used across various applications such as taxi fraud detection [208], [209], [210], [211], [215], traffic pattern analysis [202], [203], [204], [205], [207], [222], event detection [59], [61], [214], [226], and a variety of other scenarios [206], [212], [213], [218], [220], [223], [224]. Smartphones equipped with accelerometers and gyroscopes, are employed for detecting road anomalies [227], and in road pavement analysis [213]. Loop detectors are utilized for traffic pattern analysis [202], and play a role in traffic accident risk assessment [221]. Parking sensors aid in detecting parking location anomalies [225]. Data from traffic speed sensors can be used for detecting data integrity attacks [216]. For automotive sensor security, Inertial Measurement Unit (IMU) sensors are mentioned [217]. Various air quality sensors (NO, NO2, NOx, PM1, PM10, and PM2.5) are used in air pollution analysis [220].

3) LITERATURE REVIEW

AD in smart transport environments emerged as a crucial tool for urban planning and management decision-making. It equips authorities with the capacity to identify and promptly respond to abnormal traffic patterns that could potentially have negative impacts on citizens and infrastructure [201]. Smart transport AD has been extensively reviewed in previous work, this is evident through the variety of surveys that have critically examined this field [58], [201], [228]. Comprehensive reviews on AD algorithms can be found in [201], [228]. Castro et al. [58], took a closer look at transportation networks that rely on GPS data. Their focus was to understand and analyze social mobility and behavioral patterns. The authors categorized the existing literature into: a) public transport, b) smart traffic, c) social dynamics, d) operational dynamics. Djenouri et al. [201] divided existing solutions into two primary categories: a) flow outlier detection, b) trajectory outlier detection. According to the authors, traffic flow AD approaches analyze the movement of multiple objects over time, such as the quantity of passengers or vehicles entering or exiting a region per hour. Traffic trajectory AD approaches identify anomalous routes taken by vehicles from their origin to their destination [201]. Previous work on AD in intelligent transportation environments, including the algorithms used, the learning scenario and the scope of application are listed in Table 6 and discussed below.

Studies on traffic pattern analysis aim to understand and detect unusual traffic behavior, flow inconsistencies, and traffic incidents. Notable works in this domain include [202], [203], [204], [205], [206], [207], [234]. In [202], Yang and Zhou introduced a novel approach to detect abnormal traffic patterns using a combination of Locally Linear Embedding (LLE) and PCA. By applying these manifold learning techniques to traffic data obtained from over 4000 sensors, they effectively extracted features that represent traffic flow. Their method proved successful in identifying anomalies in traffic patterns that aligned with special days like New Year's Day and Independence Day, or during extreme weather conditions. Chawla et al. [203] developed a pioneering two-step approach combining PCA and L1 optimization to infer the root causes (e.g., re-routing of traffic) of road traffic anomalies. This method, applied to a vast dataset of nearly 790 million GPS points from Beijing taxis, allowed for the identification and explanation of anomalies in traffic patterns. For instance, they were able to discern traffic rerouting due to specific events like the Beijing marathon. In [204], the authors proposed a method based on the Likelihood Ratio Test (LRT) to detect emerging anomalous traffic patterns using GPS data. The approach involves analyzing GPS trajectory data from taxis to identify abnormal traffic behavior across different urban areas. Wang et al. [205] presented an approach to detect abnormal areas in Beijing by combining high-level features like passenger flow, as well as travel time from bus and taxi trajectories. The authors proposed their Spatio-Temporal Data Cube (STD) model and an improved version of the LOF algorithm for detecting areas in which abnormal traffic flow occurs. Hassan et al. [234] developed an unsupervised method based on Multi-Channel Singular Spectrum Analysis (MSSA). Their technique was effective in identifying contextual and collective traffic anomalies, applying the model to data from the Connected Vehicles and Smart Transportation (CVST) platform. Peng et al. [207] developed an unsupervised algorithm for intelligent transportation systems using the Informer and OC-SVM algorithms. They focused on detecting anomalous vehicle and pedestrian flows, applying the algorithm to a real-world dataset from Guiyang City and the public Skoltech Anomaly Benchmark (SKAB). Kaytaz et al. [206] introduced their unsupervised Competitive Learning based Anomaly Detection (CLAD) approach, combining ARIMA forecasting, CentNNs, and graph-based AD. The approach effectively analyzed multi-dimensional sensor data for detecting vehicular traffic anomalies (vehicle velocity, vehicle count per minute, and lane change activities), leveraging competitive learning for clustering.

Taxi and driving fraud detection encompasses the detection of taxi fraud, anomalous taxi trips, and dangerous driving behaviors [161], [208], [209], [210], [211], [212], [213]. Ge et al. [208] developed a taxi driving fraud detection system. Their method combines travel route and driving distance evidence, employing a parameter-free approach for the former and a generative statistical model for the latter. The integration of these evidences using Dempster-Shafer theory enables a more accurate and reliable detection of fraudulent activities by taxi drivers. In [209], Zhang et al. proposed their Isolation-Based Anomalous Trajectory (iBAT) detection method, which isolates trajectories differing significantly from the majority, using large-scale GPS data from taxis. This method is particularly effective in applications such as detecting taxi driving frauds and changes in urban road networks. Their approach, which notably achieves high performance offers a novel perspective in exploiting GPS traces for urban dynamic analysis. In [210], Chen et al. extended the work of Zhang et al. [209] by introducing their Isolation-Based Online Anomalous Trajectory Detection (iBOAT) method. This online model innovatively identifies segments of a taxi's trajectory that contribute to its anomalous nature, addressing the limitations of the previous iBAT method. Their analysis, based on extensive experiments with large-scale taxi GPS data, revealed that the majority of anomalous trajectories were due to intentional deviations from normal routes by taxi drivers committing fraud. Belhadi et al. [211] proposed an algorithm for identifying individual and group taxi trajectory frauds. Their approach, combining a phase-based algorithm and a GPU-based sliding windows strategy, was evaluated on both synthetic and real-world taxi trajectory datasets. In [212], Zhang proposed a graph-based method for detecting anomalous taxi trips in New York City. The method focused on identifying significant deviations between recorded trip distances and computed shortest paths using a NAVTEQ street map dataset. By conducting spatial and network analysis, Zhang not only identified outliers in over 166 million taxi trip records but also contributed to a deeper understanding of urban dynamics. Kieu et al. [161] proposed to enrich the features space of time series by extracting statistical features within overlapping sliding windows. Dimensionality reduction is performed on the enriched time series using an AE in order to capture representative latent features. Experiments were conducted

TABLE 6. Summary of previous work on AD in smart transport. Symbols denote learning scenarios: ○ = unsupervised, ⦿ = semi-supervised, ● = supervised. Additional symbols for anomaly types: ⊡ = point anomalies, ⊟ = context anomalies, ⊠ = collective anomalies. The literature examined predominantly employs unsupervised learning techniques (○) across various application areas. A notable aspect is the use of GPS sensors to track the position of vehicles.

Work	Year	Algorithms	Scenario	Area of Use	Sensors	Anomaly Type	Dataset
[202]	2011	LLE, PCA	○	Traffic pattern analysis	Loop detectors	⊟	Proprietary (Traffic volume and occupancy)
[208]	2011	Generative Modeling	⦿	Taxi fraud detection	GPS	⊟	Proprietary
[209]	2011	iBAT	○	Taxi fraud detection, Road network changes	GPS	⊡, ⊟	Proprietary (Hangzhou, China)
[203]	2012	PCA, L1 Optimization	⦿	Root cause of road traffic anomalies	GPS	⊟	Proprietary (Beijing taxi GPS trajectories)
[212]	2012	Graph-based method	○	Anomalous taxi trips	GPS	⊟	NYC TLC [229], NAVTEQ street map
[210]	2013	iBOAT	⦿	Taxi fraud detection	GPS	⊟	Proprietary (Hangzhou, China)
[204]	2013	LRT	○	Traffic anomalies	GPS (Taxis)	⊠	Proprietary (Beijing taxi trajectories)
[214]	2013	HMM	○	Gathering event detection	GPS	⊠	Proprietary (Japan mobile GPS)
[225]	2014	FF Clustering, SVDD, EM Clustering	○	Parking locations	Parking sensors	⊡	Proprietary (San Francisco parking)
[213]	2014	Wavelet decomposition analysis, SVM	●	Road pavement analysis	Smartphones (GPS, Accelerometer, Gyroscope)	⊡	Proprietary (Vlora, Enschede)
[61]	2015	MSLT, ST_LRT, Candidate generation algorithm	○	Gathering event detection	GPS	⊠	Taxi [229], 311 NYC complaints, Bike rental, NYC POIs
[226]	2016	Bayesian Inference, Markov model	○	Various urban anomalies	Crowdsourcing	⊟	Proprietary (311 NYC non-emergency service platform)
[223]	2016	FBTAD	○	Anomalous trajectories on road segments	GPS (Vehicles)	⊡	Brinkhoff's Generator, Beijing Taxi
[224]	2017	DB-TOD	○	Anomalous trajectories	likely GPS (Taxi)	⊡	Porto Taxi [230], Shanghai Taxi
[63]	2018	OC-SVM-rbf	○	Crowd gatherings, accidents	likely GPS (Taxi, Bike)	⊟, ⊠	Proprietary (Taxi, Bike trajectories from New York)
[161]	2018	2DCNN-AE, LSTM-AE	○	Dangerous driving behavior, hazardous roads	GPS, Accelerometer	⊡	UAH-DriveSet [231], NAB [75], Yahoo S5 [141]
[205]	2018	STD, LOF	○	Abnormal traffic flow	Smartcard, GPS (Taxi)	⊟	Proprietary (Bus, Taxi)
[59]	2019	MLP, LOF	⦿	Gathering event detection	GPS (Taxi, Bike Trips), Weather	⊟, ⊠	NYC TLC [229], Bike Trip Records, Proprietary (Weather [232])
[88]	2019	Community Detection, Dimensionality Reduction, GMM	○	Gathering event detection	N/A (Taxi, Subway)	⊟, ⊠	Proprietary (Taxi and Subway from New York, Taipei)
[215]	2020	LSTM, OC-SVM	⦿	Unusual events (concerts, traffic accidents)	GPS (Taxi, Subway)	⊟, ⊠	Proprietary (Taxi, Subway)
[216]	2019	Statistical means, Gaussian Processes	○	Data integrity attacks	Traffic speed sensors	⊡, ⊠	HERE API (Nashville, TN) [233]
[234]	2019	MSSA	○	Unusual patterns in traffic	Various	⊟, ⊠	CVST platform traffic data
[219]	2020	MO-GAN	○	Intelligent transportation system security	Not specified	⊟	Not specified
[217]	2021	HDAD	○	Automotive sensor security	CAN Bus, GPS, IMU	⊡, ⊟	AEGIS Big Data Project [235]
[211]	2021	Two-phase-based algorithm	⦿	Taxi fraud detection	GPS (taxi trajectories)	⊟, ⊠	Proprietary (synthetic and real-world taxi trajectories)
[207]	2022	Informer, OC-SVM	○	Traffic and pedestrian flow	Not specified	⊟	Guiyang vehicles and pedestrian, SKAB [236]
[222]	2022	Incremental region growing approximation	○	Traffic incident detection	TMC sensors	⊟	Nashville 2019 traffic
[218]	2022	Folded Gaussian Model, Active Learning	⦿	Sensor faults and failures	Traffic message channel sensors	⊟	Nashville vehicular
[206]	2022	ARIMA, CentNN	○	Vehicular traffic anomalies	DIGINET-PS platform sensors	⊟	DIGINET-PS traffic
[220]	2022	SparkGHSOM	○	Air pollution analysis	Air quality sensors, GPS (buses)	⊟	Air pollution, public transport (Oslo)
[221]	2023	AE (with Attention)	○	Traffic accident risk	Fixed sensors, loop detectors	⊟	Proprietary (Yan'an elevated road)

using CNN and LSTM based AEs. Anomalies such as dangerous driving behaviours are detected by deviations between the enriched and reconstructed time series. Seraj et al. [213] introduced a road pavement anomaly detector based on wavelet decomposition analysis and SVM. Their method, named RoADS uses data provided by built-in smartphone sensors in order to detect road pavement anomalies such as manholes, speed humps, patches, cracks, and potholes.

Event and gathering detection is concerned with identifying significant events and gatherings. It covers the detection of gatherings, concerts, accidents, and other unusual events. Key references in this domain include [59], [61], [63], [88], [214], [215]. Witayangkurn et al. [214] developed a framework using a HMM to detect gathering events (e.g., fireworks festivals, New Year's events) in urban areas. They processed 9.2 billion GPS records from 1.5 million individuals in Japan. According to the authors, natural events such as earthquakes most affected the occurrence of anomalous traffic trajectories. Zheng et al. [61] fuse the information from multiple urban datasets across different domains so that crowd gatherings can be detected. To address this challenge, the authors propose a method with three primary components, namely a Multiple-Source Latent-Topic (MSLT) model, a Spatio-Temporal Likelihood Ratio Test (ST_LRT), and a candidate generation algorithm. Zheng et al. [63] proposed a method for detecting urban anomalies, such as crowd gatherings, utilizing multiple spatio-temporal data sources. Their approach involves a similarity-based algorithm for individual anomaly score estimation and an OC-SVM algorithm for aggregating these scores to capture complex anomaly patterns across different data sources. He et al. [88] explored the detection of urban events, such as national holiday, cultural events, and natural disasters in urban mobility networks, evaluating traffic flow characteristics and anomalies using a pipeline approach. This method involved community detection, unsupervised dimensionality reduction, and GMMs to identify outliers in urban traffic data from New York City and Taipei. In [59], Zhang et al. presented an approach for detecting urban anomalies by decomposing urban dynamics into normal and abnormal components using a neural network that fuses spatial and temporal features. Their method identifies gatherings based on deviations from the estimated normal urban dynamics. Kong et al. [215] proposed their Hierarchical Urban Anomaly Detection (HUAD) framework, employing LSTM for predicting traffic flow and OC-SVM for detecting unusual events such as concerts, particularly focusing on taxi and subway data across various times and regions.

Transportation system security addresses security concerns in transportation systems, focusing on data integrity, sensor security, and overall system security [216], [217], [218], [219]. Wilbur et al. [216] presented a decentralized framework, focusing on real-time identification of data integrity attacks using a two-tiered approach with Roadside Units (RSUs) and Gaussian Processes. Wang et al. [217] introduced Hyperdimensional Computing-based Anomaly Detection (HDAD), a method using hyperdimensional computing for sensor spoofing attack detection in autonomous vehicles. Madhavarapu et al. [218] introduced a method utilizing a folded Gaussian model augmented with active learning. Their approach efficiently identified anomalies such as sensor faults and failures in Traffic Message Channel (TMC) sensor data, enhancing traffic management and safety in smart transportation systems. In [219], the author proposed their Multi-Objective GAN (MO-GAN) approach for intelligent transportation system security. The authors combined genetic and a GAN model, to address class imbalances within intelligent transportation systems.

Studies on environmental monitoring and public health include [220], [221], [222]. Mignone et al. [220] developed an unsupervised approach for air pollution detection in Oslo using the SparkGHSOM algorithm and various air quality sensors (NO, NO2, NOx, PM1, PM10, and PM2.5). They enhanced the algorithm for explainable AD, effectively identifying irregular patterns in air quality and traffic data. In [222], the authors propose an unsupervised incremental region growing approximation algorithm for traffic incident detection, such as fire and emergency response operations. Zhao et al. [221]. introduced an unsupervised method based on an AE with attention mechanism for Road Rraffic Accident (RTA) risk detection. The method effectively identifies RTA risk by analyzing traffic condition features and employing an enhanced loss optimization, evaluated on two real traffic datasets.

Anomalous trajectory and location detection focuses on detecting unusual patterns in trajectories and locations, such as the detection of anomalies in road trajectories and parking location [223], [224], [225], [226]. Wang et al. [223] developed their Feature-Based method for Traffic Anomaly Detection (FBTAD) method to detect traffic anomalies by analyzing features such as travel speed and traffic density. Their approach efficiently identifies anomalous trajectories on road segments by monitoring significant changes in traffic flow characteristics. Wu et al. [224] proposed a probabilistic approach for traffic trajectory AD. Their Driving Behavior based Trajectory Outlier Detection (DB-TOD) approach detects anomalous trajectories that deviate from the historical trajectory distribution. Zheng et al. [225] developed an approach for detecting anomalous car parking locations using real-time data from San Francisco. They employed algorithms such as farthest first clustering, SVDD, and expectation maximization. Huang et al. [226] introduced the Crowdsourcing-based Urban Anomaly Prediction Scheme (CUAPS), a method utilizing spatial and temporal crowdsourcing data from NYC's 311 service platform to predict various urban anomalies, including noise issues, blocked driveways, illegal conversions of residential buildings, and illegal parking.

4) DATASETS

In this section, we present an overview of the datasets that can be used for traffic AD. These datasets include data from various sources such as cameras, GPS, and other sensors, which can provide information on various aspects of traffic and activity in public spaces, such as the number and types of vehicles, the speed and direction of traffic, road conditions and the density of people in a given area. Table 7 presents an overview of these datasets, including information such as the nature of the data (whether public or otherwise), the labels associated with the data, and the number of instances.

a: UAH-DRIVESET

The UAH-DriveSet [231] is an open dataset primarily aimed at driving analysis, collected through the "DriveSafe" driving monitoring app using smartphone sensors. This dataset encompasses a wide range of variables, gathered by six drivers of varying ages and vehicles. The drivers exhibited three different behaviors that are annotated, namely normal, aggressive, and drowsy. Two different routes have been recorded: a) 25 km motorway, b) 16 km secondary road. The dataset includes over 500 minutes of realistic driving data, along with raw data and supplementary semantic information, as well as video recordings of the drives.

b: 311 SERVICE REQUESTS FROM 2010 TO PRESENT

The "311 Service Requests from 2010 to Present" dataset [237], maintained by NYC OpenData, encompasses a wide array of information related to various service requests reported within New York City. This dataset is continuously updated and falls under the category of social services. It includes a variety of tags such as city government, social services, and different types of complaints like rodent issues, bike problems, and potholes.

c: NYC TLC

The NYC TLC Trip Record Data [229], managed by the New York City Taxi and Limousine Commission (TLC), encompasses detailed trip records for yellow and green taxis, as well as for-hire vehicles (FHV). This data includes fields for pick-up and drop-off dates/times, locations, trip distances, fares, rate types, payment types, and driver-reported passenger counts for taxis. For FHV, it captures dispatching base license numbers, pick-up dates, times, and taxi zone location IDs. The dataset is updated monthly and stored in the PARQUET format since May 2022.

d: BIKE DATASET

The City Bike NYC dataset [238], provided by Citi Bike NYC, offers comprehensive data on bike trips across the city. The current format of the data includes information like ride ID, start and end times, start and end station names and IDs, as well as the latitude and longitude of these stations. Additionally, it specifies whether the ride was made by a member or a casual rider. Previously, the dataset included more detailed information such as trip duration, bike ID, user type (differentiating between short-term pass users and annual members), gender, and year of birth.

e: PORTO TAXI TRAJECTORY

The Porto Taxi Trajectory Data [230] is a comprehensive dataset that captures the trajectories of 442 taxis operating in the city of Porto, Portugal. This data was collected over a

TABLE 7. Smart transport dataset overview with general information. These datasets are characterized by their diverse data types, including GPS, textual, and numerical data, and offer extensive and continuously updated information.

Work	Dataset	Dimensionality	Data type	Area of Use	Instances	Public	Labels	Environment
[231]	UAH-DriveSet	Various	Numerical	Driving behavior analysis	$>$ 500 min of data	Yes	Yes	Motorway, Secondary road
[237]	311 Service Requests from 2010 to Present	Various	Textual data	Urban studies, city planning	Continuously updated, $>$ 20 million	Yes	No	New York City
[229]	NYC TLC	Various	Textual, numerical	Transportation studies, urban planning	Continuously updated, several billion records	Yes	No	New York City
[238]	City Bike NYC	Various	Numerical, categorical	Urban transportation, planning	Continuously updated	Yes	No	New York City
[230]	Porto Taxi Trajectory	9 features	Textual, numerical	Urban transport, traffic analysis	1710671	Yes	No	Porto, Portugal

one-year period, from July 1, 2013, to June 30, 2014. The dataset comprises over 1.7 million taxi journey entries, reflecting a significant volume of data points, specifically more than 83 million GPS data points.

Among the datasets presented in Table 7, a notable aspect is their diversity in data types such as textual, numerical, and categorical data. All of the datasets listed are publically available, although anomalies are rarely annotated [231]. Another significant characteristic of these datasets is their size and dynamic nature, with datasets like the NYC TLC [229] and City Bike NYC [238] being continuously updated, providing millions to billions of instances. This continual update feature makes these datasets particularly valuable for longitudinal studies in smart transportation environments.

C. SMART INDUSTRY

This section presents previous work on AD in industrial environments. With the increasing adoption of IIoT and Industry 4.0 technologies, industrial environments have become more complex, dynamic and data-driven. The term *smart factory* is not yet defined consistently, as other terms like U-factory, the factory of things, the factory in real time frame and the intelligent factory of the future are frequently used [239]. A smart factory is basically a collection of network enabled devices and systems that exchange information with each to automatically coordinate the fulfillment of production requirements. A Cyber-Physical System (CPS) forms the basis of a smart factory [240], and it is characterized by its high degree of complexity [241]. It typically consists of distributed computing elements, mechanical parts, and electronic parts that communicate via IT network infrastructure, such as the Internet. CPSs are augmenting critical public infrastructure [242] such as transportation, electric power generation, water treatment and distribution. In the context of Industry 4.0, these systems are increasingly automated, such that they can dynamically adapt to production requirements. The German Federal Ministry of Education and Research refers Industry 4.0 to "the intelligent networking of machines and processes for industry with the help of information and communication technology" [243]. The 2030 vision of Industry 4.0 is built on three strategic fields of action: a) Autonomy, b) Interoperability, c) Sustainability [244]. In previous work [245], an architecture was proposed, that serves as a reference for IoT-based smart factories, including an energy management scheme that increases energy efficiency by integrating energy data in production management.

1) USE CASE SCENARIOS

This section presents use cases for AD in smart industrial environments. Figure 18 visualizes a comprehensive overview of the various use cases investigated in previous research. In the following, the application areas and the particular use cases are described in further detail:

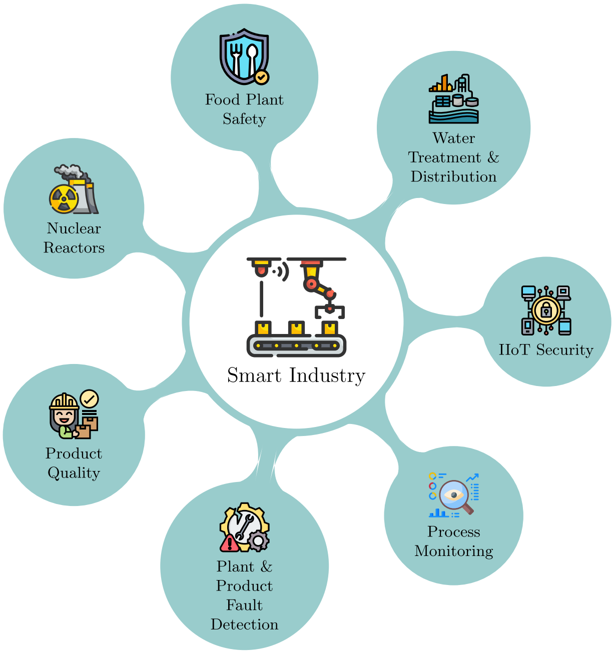


FIGURE 18. Use cases for AD in smart industry.

a: PRODUCT QUALITY INSPECTION

This category includes research focused on ensuring the quality of products through various inspection techniques. It encompasses studies on product quality inspection in various industries [246], [247], [248], quality monitoring in manufacturing [249], and industrial product surface defect detection [250].

b: INDUSTRIAL PROCESS MONITORING AND FAULT DETECTION

Emphasizing the monitoring of industrial processes and the detection of faults, this category includes works on fault detection in steel rolling mills [251], [252], assembly conveyor bearing failures [253], parts assembly failures [254], APU maintenance [255], air-blowing machine monitoring [256], research on food plant safety [257], manufacturing process failures [258], and general process monitoring [259].

c: SECURITY IN INDUSTRIAL AND IOT ENVIRONMENTS

This category addresses security concerns in industrial and IoT settings. It includes research on IIoT security [260] and intrusion detection in logistics networks [261].

d: ENERGY AND UTILITY SYSTEMS

Focusing on the monitoring and AD in energy and utility systems, this category includes studies on energy systems in the steel industry [262], water treatment and distribution systems [263], and nuclear reactors [264], [265].

2) TYPICAL SENSORS

This section presents sensors that are commonly used for AD in smart industry environments. Force sensors are used to detect assembly failures in parts assembly processes [254]. Neutron detectors are employed for monitoring nuclear reactor perturbations [264], [265]. Water treatment and distribution application involve sensors such as pressure meters and flow meters [263]. Various sensors such as accelerometers, oil pressure, temperature, current, speed, and torque sensors are used for fault detection in steel rolling mills [251], [252]. Microphones are employed for detecting assembly conveyor bearing failures [253]. Product flow, pressure (heat exchanger), and temperature sensors are utilized for food plant safety [257]. Cameras are employed for metal textile quality control [248], industrial product surface defect detection [250], and product quality inspection [247]. Gas flow sensors are utilized in the energy system of the steel industry [262].

3) LITERATURE REVIEW

This literature review focuses on the recent developments and research in the field of AD techniques for smart industry environments.

Table 8 lists a variety of applications that are discussed in the following. Product quality inspection is dedicated to ensuring product quality through various inspection techniques. It encompasses studies on quality inspection across different industries, monitoring quality in manufacturing, and detecting surface defects in industrial products. Key studies in this domain are summarized in [246], [247], [248], [249], [250]. Zhang et al. [246] introduced a method for product quality inspection using a Gradient Compensation Gaussian Restricted Boltzmann Machine (GC-GRBM). Their method was applied to white wine and cigarette product quality inspection. Tang and Jung [247] developed the Reliable Anomaly Detection and Localization (RADL) system, an approach for industrial product quality inspection, integrating a pre-trained ImageNet backbone, a Fake Defect Feature Augmentation (FDFA) strategy, and Hardness-aware Cross-Entropy loss (HCELoss). Arndt et al. [248] introduced an approach combining Patch Distribution Modeling (PaDIM) and Self-Training Feature Pyramid Matching (STFPM) algorithms to aid quality control in metal textile production. Focused on reducing cognitive load for workers, the authors aimed at identifying defects in car exhaust gas regulation filters based on high-resolution monochrome and depth images. Carletti et al. [249] proposed an unsupervised method to assess feature importance in AD, called Depth-based Isolation Forest Feature Importance (DIFFI). Liu et al. [250] introduced the Self-Updated Memory and Center Clustering (SMCC) framework for AD and localization in industrial images, employing pretrained back-bone models as feature extractors and GMM clustering. Their method was applied to industrial product surface defect detection.

Notable contributions in the field of industrial process monitoring and fault detection can be found in [251], [252], [253], [254], [255], [256], [257], [258], and [259]. Former studies, such as Rodriguez et al. [254], suggested the use of traditional machine learning algorithms. In [254], the authors employed SVM and PCA in a supervised learning scenario for failure detection in a automated parts assembly. Lindemann et al. [258] evaluated the performance of two data-driven self-learning approaches based on real data originating from hydraulic press metal forming processes. Kalør et al. [259] investigated remote AD using PCA and AE methods on resource-constrained IoT devices, and their method was applied to industrial process monitoring. Acernese et al. [251] proposed a two-step AD strategy for steel rolling mills, combining Reweighted Minimum Covariance Determinant (RMCD) and HMMs, to efficiently detect faults in a high-risk industrial setting on real production data. Sarda et al. [252] proposed a multi-step strategy for rolling mill fault detection in steel industry, utilizing RMCD and HMMs. Tanuska et al. [253] developed a system for bearing failure prediction and detection in assembly conveyors using sound analysis and MLPs. The authors trained multiple MLPs using an automated network search function. Davari et al. [255] developed a learning-based predictive maintenance framework for Air Production Units (APU), using a Sparse Autoencoder (SAE) approach. The study, focused on both analog and digital real-time sensor data. Velásquez et al. [256] developed a machine-learning ensemble integrating LOF, OCSVM, and AE for AD in industrial air-blowing machines. The authors incorporated data from numerous sensors and conducted extensive preprocessing prior to the AD process. Tancredi et al. [257] employed multiple linear regression, a multi-layer perceptron, and k-means clustering, demonstrating their efficacy in enhancing the safety of a industrial food plant pasteurization system.

Applications on security in industrial and IoT environments can be found in [260] and [261]. Demertzis et al. [260] introduced a blockchain security architecture integrating smart contracts with AEs, focusing on securing IIoT communications. Qi et al. [261] developed their Multiaspect Data Streams Anomaly Detection (MDS_AD) approach for fast anomaly identification in logistics networks, leveraging a combination of Locality-Sensitive hashing (LSH), Isolation Forest (IF), and PCA.

TABLE 8. Summary of previous work on AD in smart industrial environments. Symbols denote learning scenarios: ○ = unsupervised, ◉ = semi-supervised, ● = supervised. Additional symbols for anomaly types: ⊡ = point anomalies, ⊟ = context anomalies, ⊠ = collective anomalies. A notable aspect is the diversity of algorithms used, applied across various industrial areas, utilizing different sensor types. This diversity indicates the complexity and varied nature of industrial processes and anomalies.

Work	Year	Algorithms	Scenario	Area of Use	Sensors	Anomaly Type	Dataset
[254]	2010	SVM, PCA	●	Parts assembly failures	Force	⊡, ⊟	Proprietary (Assembly force signatures)
[265]	2018	CNN, DAE, k-means clustering	◉	Nuclear reactor perturbations	Neutron detectors	⊟	Proprietary (Core Sim [266] simulated data)
[264]	2019	DWT, CNN	○	Nuclear reactor perturbations	Neutron detectors	⊟	Proprietary (SIMULATE-3K simulated data)
[258]	2019	k-means clustering, LSTM, AE	○	Manufacturing process failures	Various	⊡	Private (hydraulic press)
[246]	2019	GC-GRBM	●	Product quality inspection	Various	⊡	Wine Quality [267], Cigarette factory data (China)
[249]	2019	IF, DIFFI	○	Quality monitoring	Not specified	⊡	Synthetic, Industrial (Pressure Profiles in Refrigerator Manufacturing)
[268]	2019	Vertex-weighted hypergraph learning	●	Various	Various	⊟	Various
[260]	2020	AE	◉	IIoT Security	Various	⊡, ⊟, ⊠	MDB Protocol Data
[259]	2021	PCA, AE	◉	Industrial Process Monitoring	Not specified	⊡, ⊟	MIMII [269]
[251]	2021	RMCD, HMM	◉	Fault detection in steel rolling mills	Accelerometers, Oil pressure, temperature, Current, Speed, Torque	⊡, ⊟	Not specified
[255]	2021	SAE, VAE	◉	APU Maintenance	Pressure, motor current, Air intake valve	⊡, ⊟	Not specified
[253]	2021	MLPs, Sound Analysis	●	Assembly conveyor bearing failures	Temperature, microphone	⊡	Proprietary
[252]	2021	RMCD, HMM	○	Rolling mill fault detection	Accelerometers, Pressure, Temperature, Current, Speed, Torque	⊡, ⊟	Not specified
[261]	2022	MDS_AD (Locality-Sensitive Hashing, Isolation Forest, PCA)	○	Intrusion detection in logistics networks	Not specified	⊡, ⊟, ⊠	UNSW-NB15 [270]
[257]	2022	Multiple Linear Regression, MLP, K-Means	●	Food plant safety	Product flow, Pressure (heat exchanger), Temperature)	⊡, ⊠	Proprietary
[263]	2022	LSTM-VAE	◉	Water treatment & distribution	Various	⊡, ⊟, ⊠	SWaT, WADI
[256]	2022	LOF, OCSVM, AE	◉	Air-blowing machines	Pressure (suction, discharge), Temperature (flow), machine vibration, RPM, Active Power, Motor current	⊡, ⊟, ⊠	Proprietary
[248]	2023	PaDIM, STFPM	◉	Metal textile quality control	Line scan camera, Laser	⊡	Proprietary
[247]	2023	RADL, FDFA, HCELoss	○	Product quality inspection	Imaging techniques	⊡, ⊟	MVTec-AD [271], Heat staking points, Small-part
[262]	2023	VHCA-DBSCAN, Modified LOF	○	Energy system in steel industry	Gas flow	⊡, ⊟, ⊠	Proprietary
[250]	2023	SMCC, GMM	○	Industrial product surface defect detection	Cameras	⊡, ⊟	MVTec AD [271]

Previous work on energy and utility systems, including studies on energy systems in the steel industry, water treatment and distribution systems, and nuclear reactors is encapsulated in [262], [263], [264] and [265]. Calivá et al. [265] proposed a deep learning approach based on a 2D CNN that detects fluctuations in nuclear reactors and localizes the point the fluctuation originates from. In [264], Tagaris et al. performed an wavelet-based analysis on changes in neutron flux in nuclear reactor cores in order to obtain scaleograms. A convolutional neural network has been trained using the scaleograms such that it can detect reactor core failures. Their methodology utilized simulated data from the SIMULATE-3K tool, focusing on in-core and ex-core neutron flux signals. Fährmann et al. [263] proposed a lightweight LSTM-VAE architecture for AD in water treatment and water distribution applications. In [262], Jin et al. introduced their Varying-scale Hypercube Accelerated Density-Based Spatial Clustering for Applications with Noise (VHCA-DBSCAN) method for AD within the steel industry. Employing Gaussian probability density estimation, along with a modified LOF for outlier evaluation.

4) DATASETS

This section provides an overview of related datasets. Unlike datasets that are generally considered for the application of AD algorithms, the availability of datasets that contain industrial sensor and actuator data is limited [272]. Table 9 presents an overview of key datasets, including information such as the nature of the data (whether public or otherwise), the labels associated with the data, and the number of instances.

a: UNSW-NB15

The UNSW-NB15 [270] dataset, intended for network intrusion detection, was created in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) at UNSW Canberra. It comprises raw network packets captured with the tcpdump tool, totaling about 100 GB in size, and stored as pcap files. It includes nine different types of attacks (i.e., Fuzzers, Analysis, Backdoors, DoS (Denial of Service), Exploits, Generic, Reconnaissance, Shellcode, and Worms).

b: MIMII

The Malfunctioning Industrial Machine Investigation and Inspection (MIMII) [269] dataset contains sounds generated from four types of industrial machines (i.e. valves, pumps, fans, and slide rails). The datasets has been captured in real factory environments and includes normal and anomalous operating conditions.

c: MVTEC AD

The MVTec AD dataset [271] is a comprehensive collection of over 5000 high-resolution images across fifteen object categories, tailored for benchmarking AD methods in industrial inspection. The dataset is enhanced with pixel-precise defect annotations.

d: SKAB

The Skoltech Anomaly Benchmark (SKAB) [236] dataset is designed for benchmarking AD algorithms. It consists of multivariate time series data from a simulated industrial control system. The dataset contains 35 individual data files, encompassing various sensor readings such as temperature and pressure. Primarily used in the area of industrial process control and monitoring, the SKAB dataset has a single labeled anomaly per data file.

e: SWAT

The Secure Water Treatment (SWaT) [276] dataset originates from a small-scale but fully functional testbed that mimics a real-world industrial facility, built at the Center for Cyber Security Research, iTrust [277]. The data collected within the SWaT testbed was accumulated over 11 days. In the last four days of data collection, 36 attack scenarios were executed [278]. The attacks carried out are reflected in the dataset by modified sensor and actuator values. The attacks targeted various attack points, including the physical sensors and actuators, as well as access points to the network

TABLE 9. Industrial dataset overview with general information. Among the datasets listed, the largest in terms of total instances is the "SMD" dataset with a total of 1416825 instances. The "MVTec AD" dataset has the highest dimensionality, with images of 2048 × 2048 resolution. For the highest percentage of anomalies, the "MIMII" dataset stands out with ∼18.86% anomalies.

Work	Dataset	Train	Test	Dimensions	Attacks	Anomalies (%)	Public	Labels	Area of Use
[273]	WADI	1048571	172801	126	16	∼5.99	Restricted	Partial	Water distribution system
[274]	BATADAL	8761/4177	2089	43	7	∼1.46	Restricted	Partial	Water distribution network
[275]	Water Storage Tank	236179	-	23	6	-	Yes	Yes	Water storage tank
[127]	SMD	708405	708420	28 × 38	-	∼4.16	Yes	Yes	Server machines
[137]	SMAP	135183	427617	55 × 25	-	∼13.13	Yes	Yes	Spacecraft
[137]	MSL	58317	73729	27 × 55	-	∼10.72	Yes	Yes	Spacecraft
[236]	SKAB	-	-	9	-	1 Instance	Yes	Yes	Industrial AD benchmarking
[271]	MVTec AD	3629	1725	2048 × 2048	-	∼6.80	Yes	Yes	Industrial inspection benchmarking
[269]	MIMII	26092	6065	16-bit, 16 kHz	-	∼18.86	Yes	Yes	Industrial failure detection
[270]	UNSW-NB15	175341	82332	49	9	-	Yes	Yes	Network intrusion detection

communication infrastructure of the CPS (e.g., the attacker sends a malicious command to an actuator). Based on the large number of possible attack points, 28 attacks focused on a single attack point, while 8 attacks focused on multiple attack points simultaneously. In some cases, the researchers performed the attacks sequentially, and in other cases, they allowed the system to normalize before the next attack was executed. Furthermore, the operational processes of the SWaT testbed are divided into six processes P1-P6. The attacks either targeted a single process or multiple processes of the testbed.

f: WADI

The Water Distribution (WADI) [273] testbed can be considered an extension of the SWaT testbed. Although the WADI testbed is similar to the SWaT testbed, it contains components such as analyzers, booster pumps, and chemical dosing systems [273].

g: BATADAL

This dataset originates from the BATtle of the Attack Detection ALgorithms (BATADAL) [274] competition. The competition aims at the proposal of cyberattack detection algorithms for industrial environments. The dataset contains samples recorded in a water distribution network that involves seven storage tanks, eleven pumps, and five valves, controlled by nine Programmable Logic Controllers (PLCs). The network was generated with the epanetCPA toolbox, which allows the injection of cyberattacks and simulates the network's response to those attacks. The dataset is split into two training sets and a testing set. The training set 1 was generated from a simulation that lasted for one year. It does not contain any attacks; all the data pertain to normal operations. The training set 2 is partially annotated and was recorded over 6 months. It contains several attacks, some of which are approximately annotated. The testing set includes 2089 records with seven attacks. It was recorded over a three-month-long period and was used to compare the performance of the algorithms.

h: SMD

The Server Machine Dataset (SMD) [127] is a comprehensive 5-week-long dataset. It comprises data from 28 different machines, each forming a separate subset for training and testing. SMD's 38 dimensions cover metrics like CPU loads, network usage, and memory usage, making it a vital multivariate time series dataset for AD in industrial environments.

The datasets presented in Table 9, encompass a diverse range of industrial applications, including water distribution, server machines, spacecraft, and network intrusion, highlighting the varied nature of industrial processes and anomalies. They vary in data types, featuring sensor readings, network packets, as well as industrial machine sounds. These datasets focus on different types of anomalies, some with detailed annotations, reflecting the complex and specialized requirements of industrial AD. The mix of public and restricted datasets indicates a balance between open-source data availability and the need for security sensitive contexts. This diversity illustrates the evolving and nuanced challenges faced in industrial AD research.

VIII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

The rapid evolution of these smart environments, spanning across domains like smart homes, smart transportation, and smart industry, brings forth unique challenges and unexplored territories, particularly in the realm of AD. This section discusses existing gaps across these three key domains, proposing future research directions.

A. SMART HOME APPLICATIONS

Smart home environments present unique challenges, particularly in capturing the complex interactions of multiple inhabitants. Current datasets predominantly focus on single-inhabitant scenarios, limiting the scope of AD applications. The suggested future research directions are visualized in Figure 19 and described in the following.

1) MULTI-INHABITANT DATA COLLECTION

There is a significant need for datasets that capture interactions among multiple inhabitants. This would enable the development of applications like conflict detection in resource usage (e.g., simultaneous demand for heating and cooling in different rooms), or health monitoring systems that distinguish between individuals' activities and provide personalized alerts.

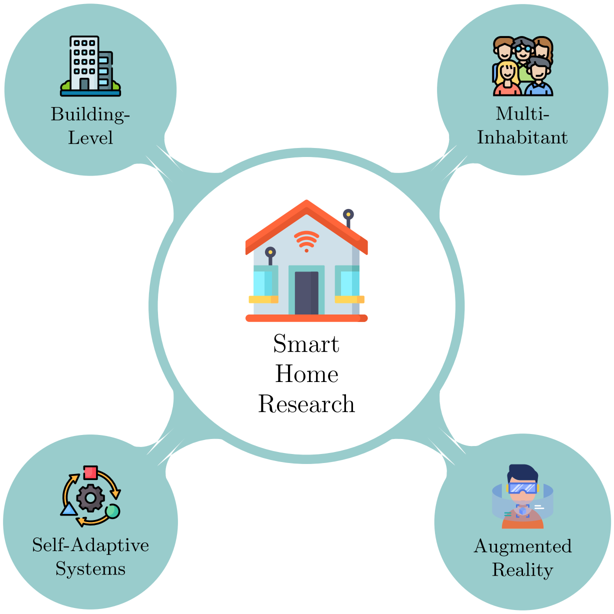


FIGURE 19. Future research perspectives for smart home AD.

2) BUILDING-LEVEL ANOMALY DETECTION

Public datasets from multiple homes could aid in detecting building-wide anomalies, such as power outages or pipe bursts. Further applications might include detecting unusual patterns in energy consumption indicative of electrical faults or proactive maintenance needs in building infrastructure.

3) SELF-ADAPTIVE SYSTEMS

Research could focus on creating self-adaptive systems that continuously learn and adjust to new patterns and behaviors in smart homes. These systems would dynamically update their models, thereby maintaining effectiveness even as household routines and environmental conditions change over time. This would be particularly relevant for adapting to lifestyle changes, seasonal variations, or the introduction of new smart home devices.

4) INTEGRATION OF AUGMENTED REALITY

Exploring the use of AR technologies to visualize anomalies in the smart home environment is a cutting-edge research direction. This could involve developing AR applications that overlay real-time data and anomaly alerts over the physical environment, providing homeowners with intuitive and interactive ways to understand and respond to anomalies.

B. SMART TRANSPORT APPLICATIONS

The diversity of transportation modes and the varied spatial and temporal granularity of datasets collected by different agencies pose challenges in forming a cohesive understanding of urban dynamics. The suggested future research directions are visualized in Figure 20 and described in the following.

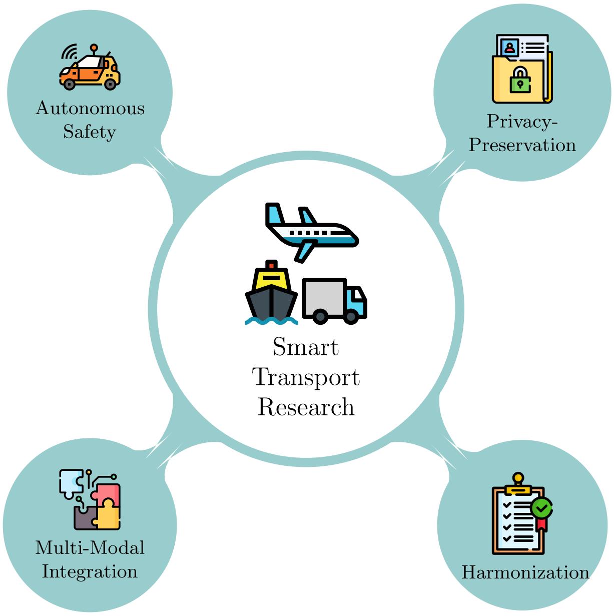


FIGURE 20. Future research perspectives for smart transport AD.

1) INTEGRATED MULTI-MODAL TRANSPORTATION DATA

Developing datasets that integrate various transportation modes (taxis, buses, trams, bikes) can provide a more holistic view of city dynamics, aiding in efficient urban planning and congestion management.

2) HARMONIZING DATA COLLECTION

Efforts to standardize the spatiotemporal granularity of data across agencies could facilitate real-time data integration and analysis.

3) PRIVACY-PRESERVING DATA COLLECTION

Innovative approaches are needed to collect detailed spatial data without infringing on individual privacy, possibly using anonymization techniques or differential privacy methods.

4) AUTONOMOUS VEHICLE SAFETY

Beyond traffic analysis, there's potential for detecting anomalies in autonomous vehicles, such as recognizing unexpected pedestrian behaviors or road blockages. Additional applications could include real-time monitoring of vehicle health and predictive maintenance alerts.

C. SMART INDUSTRY APPLICATIONS

Industrial environments, particularly power plants, pose challenges due to the vast number of sensors and the complexity of determining the source of anomalies. The suggested future research directions are visualized in Figure 21 and described in the following.

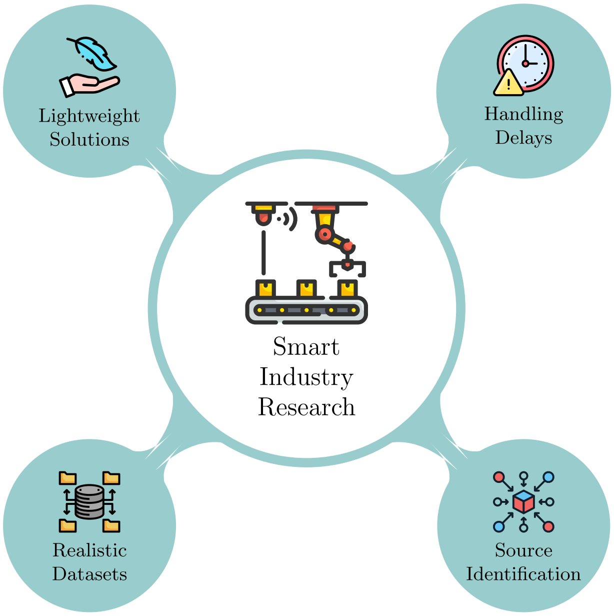


FIGURE 21. Future research perspectives for smart industry AD.

1) REALISTIC INDUSTRIAL DATASETS

There is a need for more comprehensive datasets that accurately reflect the complexity of industrial environments, to enhance the realism and applicability of AD models.

2) SOURCE IDENTIFICATION OF ANOMALIES

Future research should focus on pinpointing the exact source of an anomaly within a network of interconnected sensors, improving the precision of diagnostic systems.

3) HANDLING DATA TRANSMISSION DELAYS

Addressing the delays in data transmission due to distributed sensors and varied communication channels is crucial. Research could focus on developing models that account for these delays to ensure accurate real-time AD.

4) SCALABLE AND LIGHTWEIGHT SOLUTIONS FOR INDUSTRIAL APPLICATIONS

The presence of vast arrays of sensors and distributed infrastructures in industrial environments presents unique challenges. Industrial environments often comprise computational instances with limited computational power (e.g., PLCs), necessitating solutions that are not only scalable but also lightweight. The scalability ensures that the solution can handle the extensive data generated by numerous sensors, while the lightweight nature allows for deployment, adaptability and efficient operation even in devices with constrained computational resources [263].

IX. CONCLUSION

In this survey, we have comprehensively explored applications of AD in smart environments, particularly focusing on smart home, smart transport, and smart industry domains. We have discussed the advancements in deep learning-based AD techniques and their significant role in enhancing the safety and security of these smart environments. This survey has also delved into a variety of datasets used in these domains, emphasizing their importance in developing and evaluating effective AD algorithms.

This work investigated recent applications of AD in these domains, highlighting the critical need for robust and efficient AD systems. In smart homes, the focus lies on ensuring safety and comfort of residents through monitoring daily activities and utility usages. In smart transport, the emphasis lies on ensuring the smooth and safe operation of various transportation modes, including public transit systems, public gatherings, and overall infrastructure security. In smart industry, AD plays a pivotal role in maintaining the integrity and efficiency of industrial processes, which often involve complex machinery and extensive sensor networks. Future research directions emphasize the need for scalable and lightweight solutions. These solutions are necessary to adapt to environments with instances of limited computational power, ensuring efficient and real-time AD.

This survey presents a detailed overview of the state-of-the-art in AD techniques across key smart environments, serving as a valuable resource for researchers and practitioners in the field. The advancements in AD technologies and their diverse applications underscore their significance in the ever-evolving landscape of smart environments. As these technologies continue to develop, they will undoubtedly play an increasingly vital role in shaping the future of smart cities, improving the quality of services for citizens and ensuring the safety of individuals, as well as the security of infrastructure.

REFERENCES

[1] G. Vial, "Understanding digital transformation: A review and a research agenda," *J. Strategic Inf. Syst.*, vol. 28, no. 2, pp. 118–144, Jun. 2019, doi: 10.1016/j.jsis.2019.01.003.

[2] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-Things-based smart environments: State of the art, taxonomy, and open research challenges," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 10–16, Oct. 2016, doi: 10.1109/MWC.2016.7721736.

[3] B. Fu, N. Damer, F. Kirchbuchner, and A. Kuijper, "Sensing technology for human activity recognition: A comprehensive survey," *IEEE Access*, vol. 8, pp. 83791–83820, 2020, doi: 10.1109/ACCESS.2020.2991891.

[4] M. Ghafurian, K. Wang, I. Dhode, M. Kapoor, P. P. Morita, and K. Dautenhahn, "Smart home devices for supporting older adults: A systematic review," *IEEE Access*, vol. 11, pp. 47137–47158, 2023.

[5] K. Haricha, A. Khiat, Y. Issaoui, A. Bahnasse, and H. Ouajji, "Recent technological progress to empower smart manufacturing: Review and potential guidelines," *IEEE Access*, vol. 11, pp. 77929–77951, 2023.

[6] M. Swan, "Sensor mania! The Internet of Things, wearable computing, objective metrics, and the quantified self 2.0," *J. Sensor Actuator Netw.*, vol. 1, no. 3, pp. 217–253, Nov. 2012, doi: 10.3390/jsan1030217.

[7] E. Wartella, V. Rideout, H. Montague, L. Beaudoin-Ryan, and A. Lauricella, "Teens, health and technology: A national survey," *Media Commun.*, vol. 4, no. 3, pp. 13–23, Jun. 2016.

[8] A. E. Chung, A. C. Skinner, S. E. Hasty, and E. M. Perrin, "Tweeting to health: A novel mhealth intervention using fitbits and Twitter to foster healthy lifestyles," *Clin. Pediatrics*, vol. 56, no. 1, pp. 26–32, Jan. 2017.

[9] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Security and privacy in your smart city," in *Proc. Barcelona Smart Cities Congr.*, vol. 292, 2011.

[10] R. She, S. Liu, S. Wan, K. Xiong, and P. Fan, "Importance of small probability events in big data: Information measures, applications, and challenges," *IEEE Access*, vol. 7, pp. 100363–100382, 2019, doi: 10.1109/ACCESS.2019.2926518.

[11] M. Agyemang, K. Barker, and R. Alhajj, "A comprehensive survey of numeric and symbolic outlier mining techniques," *Intell. Data Anal.*, vol. 10, no. 6, pp. 521–538, Nov. 2006. [Online]. Available: http://content.iospress.com/articles/intelligent-data-analysis/ida00266

[12] V. Chandola, A. Banerjee, and V. Kumar, "Outlier detection: A survey," *ACM Comput. Surv.*, vol. 41, pp. 1–15, Aug. 2007.

[13] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541882.

[14] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, May 2012, doi: 10.1109/TKDE.2010.235.

[15] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier detection for temporal data: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2250–2267, Sep. 2014, doi: 10.1109/TKDE.2013.184.

[16] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," *Data Mining Knowl. Discovery*, vol. 29, no. 3, pp. 626–688, May 2015, doi: 10.1007/s10618-014-0365-y.

[17] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.

[18] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: A review," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–38, Mar. 2022, doi: 10.1145/3439950.

[19] M. Zhang, T. Li, Y. Yu, Y. Li, P. Hui, and Y. Zheng, "Urban anomaly analytics: Description, detection, and prediction," *IEEE Trans. Big Data*, vol. 8, no. 3, pp. 809–826, Jun. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9080109/

[20] L. Ruff, J. R. Kauffmann, R. A. Vandermeulen, G. Montavon, W. Samek, M. Kloft, T. G. Dietterich, and K.-R. Müller, "A unifying review of deep and shallow anomaly detection," *Proc. IEEE*, vol. 109, no. 5, pp. 756–795, May 2021, doi: 10.1109/JPROC.2021.3052449.

[21] V. R. Jakkula and D. J. Cook, "Detecting anomalous sensor events in smart home data for enhancing the living experience," in *Proc. Conquest Complex. Artif. Intell. Smarter Living AAAI Workshop*, vol. WS-11-07, San Francisco, CA, USA, Aug. 2011. [Online]. Available: http://www.aaai.org/ocs/index.php/WS/AAAIW11/paper/view/3889

[22] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[23] D. J. Cook and S. K. Das, "How smart are our environments? An updated look at the state of the art," *Pervas. Mobile Comput.*, vol. 3, no. 2, pp. 53–73, Mar. 2007, doi: 10.1016/j.pmcj.2006.12.001.

[24] SOFTEQ. (Dec. 2023). *Technologien Und Trends, Die IoT im Jahr 2020 Einen Dringend Benötigten Schub Geben*. [Online]. Available: https://www.softeq.com/de/blog/technologien-und-trends-die-iot-im-jahr-2020-einen-dringend-ben

[25] Statista. (Dec. 2023). *Forecast End-user Spending on Iot Solutions Worldwide From 2017 to 2025*. [Online]. Available: https://www.statista.com/statistics/976313/global-iot-market-size

[26] Markets and Markets. (Dec. 2023). *Smart Cities Market*. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html

[27] (2026). *Smart Cities Market by Focus Area, Smart Transportation, Smart Buildings, Smart Utilities, Smart Citizen Services (Public Safety, Smart Healthcare, Smart Education, Smart Street Lighting, and E-Governance), and Region—Global Forecast to 2026*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html

[28] Z. M. Research. (Dec. 2023). *Global Smart City Market*. [Online]. Available: https://www.zionmarketresearch.com/report/smart-cities-market

[29] M. Al-Bahri, A. Yankovsky, A. Borodin, and R. Kirichek, "Testbed for identify iot-devices based on digital object architecture," in *Proc. 18th Int. Conf. Internet Things, Smart Spaces, Next Gener. Netw. Syst. (NEW2AN)*, in Lecture Notes in Computer Science, vol. 11118, Russia, O. Galinina, S. Andreev, S. I. Balandin, and Y. Koucheryavy, Eds. Cham, Switzerland: Springer, 2018, pp. 129–137, doi: 10.1007/978-3-030-01168-0_12.

[30] *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology

[31] N. I. Council. (Dec. 2023). *Disruptive Civil Technologies*. [Online]. Available: https://irp.fas.org/nic/disruptive.pdf

[32] *Unlocking the Full Life-Cycle Value From Connected-Car Data*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data

[33] A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102886, doi: 10.1016/j.jnca.2020.102886.

[34] United Nations. (2017). *World Population Ageing*. [Online]. Available: https://www.un.org/en/development/desa/population/publications/pdf/ageing/WPA2017Highlights.pdf

[35] World Health Organisation. (Dec. 2023). *Ageing and Health*. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health

[36] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A neural network based database mining system for credit card fraud detection," in *Proc. IEEE/IAFE Comput. Intell. for Financial Eng. (CIFEr)*, Mar. 1997, pp. 220–226, doi: 10.1109/CIFER.1997.618940.

[37] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "A comparative study of anomaly detection techniques for smart city wireless sensor networks," *Sensors*, vol. 16, no. 6, p. 868, Jun. 2016, doi: 10.3390/s16060868.

[38] R. Fujimaki, T. Yairi, and K. Machida, "An approach to spacecraft anomaly detection problem using kernel feature space," in *Proc. 11th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Chicago, IL, USA, R. Grossman, R. J. Bayardo, and K. P. Bennett, Eds., Aug. 2005, pp. 401–410, doi: 10.1145/1081870.1081917.

[39] Y. K. Takehisa Yairi, "Telemetry-mining: A machine learning approach to anomaly detection and fault diagnosis for space systems," in *Proc. 2nd IEEE Int. Conf. Space Mission Challenges Inf. Technol. (SMC-IT)*, Jul. 2006, pp. 466–476.

[40] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *J. Netw. Comput. Appl.*, vol. 68, pp. 90–113, Jun. 2016, doi: 10.1016/j.jnca.2016.04.007.

[41] G. Jain, D. J. Cook, and V. Jakkula, "Monitoring health by detecting drifts and outliers for a smart environment," in *Proc. Int. Conf. Smart Homes Health Telematics*, 2006.

[42] V. Jakkula and D. J. Cook, "Anomaly detection using temporal data mining in a smart home environment," *Methods Inf. Med.*, vol. 47, no. 1, pp. 70–75, Jan. 2008. [Online]. Available: http://www.thieme-connect.de/DOI/DOI?10.3414/ME9103

[43] H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, "A survey on health monitoring systems for health smart homes," *Int. J. Ind. Ergonom.*, vol. 66, pp. 26–56, Jul. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0169814117300082

[44] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in *Proc. 31rst AAAI Conf. Artif. Intell.*, San Francisco, CA, USA. AAAI Press, Feb. 2017. [Online]. Available: http://aaai.org/ocs/index.php/WS/AAAIW17/paper/view/15126

[45] C. Douligeris and D. N. Serpanos, *Network Security: Current Status and Future Directions*. Hoboken, NJ, USA: Wiley, Jun. 2007, doi: 10.1002/0470099747.

[46] C. C. Aggarwal, "An introduction to outlier analysis," in *Outlier Analysis*. Cham, Switzerland: Springer, 2013, pp. 1–40.

[47] D. M. Hawkins, *Identification of Outliers*. Dordrecht, The Netherlands: Springer, 1980, doi: 10.1007/978-94-015-3994-4.

[48] V. Barnett and T. Lewis, "Outliers in statistical data," in *Proc. OSD*, 1984.

[49] T. Egner, J. M. Monti, and C. Summerfield, "Expectation and surprise determine neural population responses in the ventral visual stream," *J. Neurosci.*, vol. 30, no. 49, pp. 16601–16608, Dec. 2010.

[50] M. Markou and S. Singh, "Novelty detection: A review—Part 1: Statistical approaches," *Signal Process.*, vol. 83, no. 12, pp. 2481–2497, Dec. 2003.

[51] M. Markou and S. Singh, "Novelty detection: A review—Part 2: Neural network based approaches," *Signal Process.*, vol. 83, no. 12, pp. 2499–2521, Dec. 2003. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0165168403002032

[52] M. Salehi and L. Rashidi, "A survey on anomaly detection in evolving data: [With application to forest fire risk prediction]," *ACM SIGKDD Explorations Newslett.*, vol. 20, no. 1, pp. 13–23, May 2018, doi: 10.1145/3229329.3229332.

[53] C. C. Aggarwal, *Outlier Analysis*. Cham, Switzerland: Springer, 2013, doi: 10.1007/978-1-4614-6396-2.

[54] C. Commons. (2024). *Attribution-ShareAlike 4.0 International*. [Online]. Available: https://creativecommons.org/licenses/by-sa/4.0/

[55] H. M and S. M. N, "A review on evaluation metrics for data classification evaluations," *Int. J. Data Mining Knowl. Manage. Process*, vol. 5, no. 2, pp. 1–11, Mar. 2015.

[56] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006, doi: 10.1016/j.patrec.2005.10.010.

[57] J. Davis and M. Goadrich, "The relationship between precision-recall and ROC curves," in *Proc. 23rd Int. Conf. Mach. Learn. (ICML)*, in International Conference Proceeding Series, Pittsburgh, PA, USA, W. W. Cohen and A. W. Moore, Eds. New York, NY, USA: ACM, 2006, pp. 233–240, doi: 10.1145/1143844.1143874.

[58] P. S. Castro, D. Zhang, C. Chen, S. Li, and G. Pan, "From taxi GPS traces to social and community dynamics," *ACM Comput. Surveys*, vol. 46, no. 2, pp. 1–34, Nov. 2013, doi: 10.1145/2543581.2543584.

[59] M. Zhang, T. Li, H. Shi, Y. Li, and P. Hui, "A decomposition approach for urban anomaly detection across spatiotemporal data," in *Proc. 28th Int. Joint Conf. Artif. Intell.*, Macao, China, Aug. 2019, pp. 6043–6049, doi: 10.24963/ijcai.2019/837.

[60] M. Zhang, T. Li, Y. Yu, Y. Li, P. Hui, and Y. Zheng, "Urban anomaly analytics: Description, detection, and prediction," 2020, *arXiv:2004.12094*.

[61] Y. Zheng, H. Zhang, and Y. Yu, "Detecting collective anomalies from multiple spatio-temporal datasets across different domains," in *Proc. 23rd SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst.*, Bellevue, WA, USA, Nov. 2015, p. 2, doi: 10.1145/2820783.2820813.

[62] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *J. Big Data*, vol. 6, no. 1, p. 27, Dec. 2019. [Online]. Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0192-5

[63] H. Zhang, Y. Zheng, and Y. Yu, "Detecting urban anomalies using multiple spatio-temporal data sources," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 1, pp. 1–18, Mar. 2018, doi: 10.1145/3191786.

[64] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," *ACM Trans. Knowl. Discov. Data*, vol. 6, no. 1, pp. 3:1–3:39, Mar. 2012.

[65] H.-P. Kriegel, P. Kröger, and A. Zimek, "Clustering high-dimensional data," *ACM Trans. Knowl. Discovery Data*, vol. 3, no. 1, pp. 1–58, Mar. 2009, doi: 10.1145/1497577.1497578.

[66] D. Fährmann, N. Jorek, N. Damer, F. Kirchbuchner, and A. Kuijper, "Double deep Q-learning with prioritized experience replay for anomaly detection in smart environments," *IEEE Access*, vol. 10, pp. 60836–60848, 2022, doi: 10.1109/ACCESS.2022.3179720.

[67] Q. Wen, Z. Zhang, Y. Li, and L. Sun, "Fast RobustSTL: Efficient and robust seasonal-trend decomposition for time series with complex patterns," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*. New York, NY, USA: Association for Computing Machinery, Aug. 2020, pp. 2203–2213.

[68] Q. Wen, J. Gao, X. Song, L. Sun, H. Xu, and S. Zhu, "RobustSTL: A robust seasonal-trend decomposition algorithm for long time series," 2018, *arXiv:1812.01767*.

[69] A. Dokumentov and R. J. Hyndman, "STR: Seasonal-trend decomposition using regression," 2020, *arXiv:2009.05894*.

[70] J. Hansen, M. Sato, R. Ruedy, K. Lo, D. W. Lea, and M. Medina-Elizade, "Global temperature change," *Proc. Nat. Acad. Sci. USA*, vol. 103, no. 39, pp. 14288–14293, Sep. 2006.

[71] J. Yang, Z. Yue, and Y. Yuan, "Deep probabilistic graphical modeling for robust multivariate time series anomaly detection with missing data," *Rel. Eng. Syst. Saf.*, vol. 238, Oct. 2023, Art. no. 109410.

[72] C. I. Challu, P. Jiang, Y. N. Wu, and L. Callot, "Deep generative model with hierarchical latent factors for time series anomaly detection," in *Proc. 25th Int. Conf. Artif. Intell. Statist.*, May 2022, pp. 1643–1654.

[73] J. Li, S. Di, Y. Shen, and L. Chen, "FluxEV: A fast and effective unsupervised framework for time-series anomaly detection," in *Proc. 14th ACM Int. Conf. Web Search Data Mining*. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 824–832.

[74] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PLoS ONE*, vol. 11, no. 4, Apr. 2016, Art. no. e0152173. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0152173

[75] A. Lavin and S. Ahmad, "Evaluating real-time anomaly detection algorithms—The Numenta Anomaly Benchmark," in *Proc. IEEE 14th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2015, pp. 38–44.

[76] R. Wu and E. J. Keogh, "Current time series anomaly detection benchmarks are flawed and are creating the illusion of progress (extended abstract)," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, May 2022, pp. 1479–1480.

[77] G. L. Peterson and B. T. McBride, "The importance of generalizability for anomaly detection," *Knowl. Inf. Syst.*, vol. 14, no. 3, pp. 377–392, Mar. 2008.

[78] N. Han, S. Gao, J. Li, X. Zhang, and J. Guo, "Anomaly detection in health data based on deep learning," in *Proc. Int. Conf. Netw. Infrastructure Digit. Content (IC-NIDC)*, Aug. 2018, pp. 188–192.

[79] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016.

[80] B. Zhou, J. Pei, and W. Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," *ACM SIGKDD Explorations Newslett.*, vol. 10, no. 2, pp. 12–22, Dec. 2008.

[81] A. Majeed and S. Lee, "Anonymization techniques for privacy preserving data publishing: A comprehensive survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021.

[82] J. H. Huh, S. Kwag, I. Kim, A. Popov, Y. Park, G. Cho, J. Lee, H. Kim, and C.-H. Lee, "On the long-term effects of continuous keystroke authentication: Keeping user frustration low through behavior adaptation," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, no. 2, pp. 58:1–58:32, Jun. 2023.

[83] J. Druce, M. Harradon, and J. Tittle, "Explainable artificial intelligence (XAI) for increasing user trust in deep reinforcement learning driven autonomous systems," 2021, *arXiv:2106.03775*.

[84] D. Gunning, M. Stefik, J. Choi, T. Miller, S. Stumpf, and G.-Z. Yang, "XAI—Explainable artificial intelligence," *Sci. Robot.*, vol. 4, no. 37, Dec. 2019, Art. no. eaay7120.

[85] J. Chin, V. Callaghan, and S. B. Allouch, "The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective," *J. Ambient Intell. Smart Environ.*, vol. 11, no. 1, pp. 45–69, Jan. 2019.

[86] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation* (Lecture Notes in Computer Science), M. Agrawal, D. Du, Z. Duan, and A. Li, Eds. Berlin, Germany: Springer, 2008, pp. 1–19.

[87] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation*. Cambridge, U.K.: Cambridge Univ. Press, Jul. 2015.

[88] M. He, S. Pathak, U. Muaz, J. Zhou, S. Saini, S. Malinchik, and S. Sobolevsky, "Pattern and anomaly detection in urban temporal networks," 2019, *arXiv:1912.01960*.

[89] K. Sohn, C. Li, J. Yoon, M. Jin, and T. Pfister, "Learning and evaluating representations for deep one-class classification," in *Proc. 9th Int. Conf. Learn. Represent. (ICLR)*, May 2021. [Online]. Available: https://openreview.net/forum?id=HCSgyPUfeDj

[90] J. An and S. Cho, "Variational autoencoder based anomaly detection using reconstruction probability," SNU Data Mining Center, Tech. Rep., 2015.

[91] X. Gu, L. Akoglu, and A. Rinaldo, "Statistical analysis of nearest neighbor methods for anomaly detection," in *Proc. Adv. Neural Inf. Process. Syst., Annu. Conf. Neural Inf. Process. Syst.*, Vancouver, BC, Canada, H. M. Wallach, H. Larochelle, A. Beygelzimer, F. d'Alché-Buc, E. B. Fox, and R. Garnett, Eds., Dec. 2019, pp. 10921–10931. [Online]. Available: https://proceedings.neurips.cc/paper/2019/hash/805163a0f0f128e473726ccda5f91bac-Abstract.html

[92] X. Yue, C. Wang, Y. Wang, L. Chen, W. Wang, and Y. Lei, "Gas flow meter anomaly data detection based on fused LOF-DBSCAN algorithm," in *Proc. 11th Int. Conf. Comput. Pattern Recognit.*, Beijing, China, Nov. 2022, pp. 503–508, doi: 10.1145/3581807.3581881.

[93] I. T. Jolliffe, *Principal Component Analysis* (Springer Series in Statistics). New York, NY, USA: Springer, 1986, doi: 10.1007/978-1-4757-1904-8.

[94] G. Liu, Z. Lin, S. Yan, J. Sun, Y. Yu, and Y. Ma, "Robust recovery of subspace structures by low-rank representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 1, pp. 171–184, Jan. 2013, doi: 10.1109/TPAMI.2012.88.

[95] D. Reynolds, "Gaussian mixture models," in *Encyclopedia of Biometrics*. Boston, MA, USA: Springer, 2009, pp. 659–663. [Online]. Available: http://link.springer.com/10.1007/978-0-387-73003-5

[96] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF," *ACM SIGMOD Rec.*, vol. 29, no. 2, pp. 93–104, Jun. 2000. [Online]. Available: http://portal.acm.org/citation.cfm?doid=335191.335388

[97] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," in *Proc. 2nd Int. Conf. Knowl. Discovery Data Mining*. AAAI Press, 1996, pp. 226–231.

[98] R. J. G. B. Campello, D. Moulavi, A. Zimek, and J. Sander, "Hierarchical density estimates for data clustering, visualization, and outlier detection," *ACM Trans. Knowl. Discovery from Data*, vol. 10, no. 1, pp. 1–51, Jul. 2015, doi: 10.1145/2733381.

[99] H. Ringberg, A. Soule, J. Rexford, and C. Diot, "Sensitivity of PCA for traffic anomaly detection," in *Proc. ACM SIGMETRICS Int. Conf. Meas. Model. Comput. Syst.*, San Diego, CA, USA, L. Golubchik, M. H. Ammar, and M. Harchol-Balter, Eds. New York, NY, USA: ACM, Jun. 2007, pp. 109–120, doi: 10.1145/1254882.1254895.

[100] E. J. Candès, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis?" *J. ACM*, vol. 58, no. 3, pp. 1–37, May 2011, doi: 10.1145/1970392.1970395.

[101] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proc. MLSDA 2nd Workshop Mach. Learn. Sensory Data Anal.*, Gold Coast, QLD, Australia, A. Rahman, J. D. Deng, and J. Li, Eds., Dec. 2014, p. 4, doi: 10.1145/2689746.2689747.

[102] R. Chalapathy, A. K. Menon, and S. Chawla, "Robust, deep and inductive anomaly detection," in *Proc. Eur. Conf. Mach. Learn. Knowl. Discovery Databases (ECML PKDD)*, in Lecture Notes in Computer Science, vol. 10534, M. Ceci, J. Hollmén, L. Todorovski, C. Vens, and S. Dzeroski, Eds. Springer, Aug. 2017, pp. 36–51, doi: 10.1007/978-3-319-71249-9_3.

[103] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Halifax, NS, Canada, Aug. 2017, pp. 665–674, doi: 10.1145/3097983.3098052.

[104] T. Schlegl, P. Seebóck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *Proc. Int. Conf. Inf. Process. Med. Imag.*, May 2017, pp. 146–157.

[105] J. Li, J. Jia, and D. Xu, "Unsupervised representation learning of image-based plant disease with deep convolutional generative adversarial networks," in *Proc. 37th Chin. Control Conf. (CCC)*, Jul. 2018.

[106] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "GANomaly: Semi-supervised anomaly detection via adversarial training," in *Proc. 14th Asian Conf. Comput. Vis.*, in Lecture Notes in Computer Science, vol. 11363, Perth, WA, Australia, C. V. Jawahar, H. Li, G. Mori, and K. Schindler, Eds. Springer, Dec. 2018, pp. 622–637, doi: 10.1007/978-3-030-20893-6_39.

[107] B. Zong, Q. Song, M. R. Min, W. Cheng, C. Lumezanu, D. Cho, and H. Chen, "Deep autoencoding Gaussian mixture model for unsupervised anomaly detection," in *Proc. 6th Int. Conf. Learn. Represent. (ICLR)*, Vancouver, BC, Canada, Apr. 2018. [Online]. Available: https://openreview.net/forum?id=BJJLHbb0-

[108] H. Zenati, C. Sheng Foo, B. Lecouat, G. Manek, and V. R. Chandrasekhar, "Efficient GAN-based anomaly detection," 2018, *arXiv:1802.06222*.

[109] J. Donahue, P. Krähenbühl, and T. Darrell, "Adversarial feature learning," 2016, *arXiv:1605.09782*.

[110] R. Chalapathy, A. K. Menon, and S. Chawla, "Anomaly detection using one-class neural networks," 2018, *arXiv:1802.06360*.

[111] P. C. Ngo, A. A. Winarto, C. K. L. Kou, S. Park, F. Akram, and H. K. Lee, "Fence GAN: Towards better anomaly detection," in *Proc. IEEE 31st Int. Conf. Tools with Artif. Intell. (ICTAI)*, Portland, OR, USA, Nov. 2019, pp. 141–148, doi: 10.1109/ICTAI.2019.00028.

[112] T. Schlegl, P. Seeböck, S. M. Waldstein, G. Langs, and U. Schmidt-Erfurth, "F-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks," *Med. Image Anal.*, vol. 54, pp. 30–44, May 2019, doi: 10.1016/j.media.2019.01.010.

[113] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein generative adversarial networks," in *Proc. Int. Conf. Mach. Learn.*, in Proceedings of Machine Learning Research, vol. 70, D. Precup and Y. W. Teh, Eds., 2017, pp. 214–223. [Online]. Available: http://proceedings.mlr.press/v70/arjovsky17a.html

[114] S. Akçay, A. Atapour-Abarghouei, and T. P. Breckon, "Skip-GANomaly: Skip connected and adversarially trained encoder–decoder anomaly detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Budapest, Hungary, Jul. 2019, pp. 1–8, doi: 10.1109/IJCNN.2019.8851808.

[115] L. Beggel, M. Pfeiffer, and B. Bischl, "Robust anomaly detection in images using adversarial autoencoders," in *Proc. Mach. Learn. Knowl. Discovery Databases, Eur. Conf.*, in Lecture Notes in Computer Science, Würzburg, Germany, U. Brefeld, É. Fromont, A. Hotho, A. J. Knobbe, M. H. Maathuis, and C. Robardet, Eds. Springer, Sep. 2019, pp. 206–222, doi: 10.1007/978-3-030-46150-8_13.

[116] P. Perera and V. M. Patel, "Learning deep features for one-class classification," *IEEE Trans. Image Process.*, vol. 28, no. 11, pp. 5450–5463, Nov. 2019, doi: 10.1109/TIP.2019.2917862.

[117] T. Li, Z. Wang, S. Liu, and W.-Y. Lin, "Deep unsupervised anomaly detection," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Waikoloa, HI, USA, Jan. 2021, pp. 3635–3644, doi: 10.1109/WACV48630.2021.00368.

[118] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, Jul. 2006.

[119] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, "Adversarial autoencoders," 2015, *arXiv:1511.05644*.

[120] D. P Kingma and M. Welling, "Auto-encoding variational Bayes," 2013, *arXiv:1312.6114*.

[121] E. Candés, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis: Recovering low-rank matrices from sparse errors," in *Proc. IEEE Sensor Array Multichannel Signal Process. Workshop*, Oct. 2010, pp. 201–204.

[122] B. Yang, X. Fu, N. D. Sidiropoulos, and M. Hong, "Towards K-means-friendly spaces: Simultaneous deep learning and clustering," in *Proc. 34th Int. Conf. Mach. Learn.*, vol. 70, 2017, pp. 3861–3870.

[123] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, pp. 139–144, Oct. 2020, doi: 10.1145/3422622.

[124] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Venice, Italy, Oct. 2017, pp. 2242–2251, doi: 10.1109/ICCV.2017.244.

[125] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," 2015, *arXiv:1511.06434*.

[126] C. Zhang, D. Song, Y. Chen, X. Feng, C. Lumezanu, W. Cheng, J. Ni, B. Zong, H. Chen, and N. V. Chawla, "A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data," in *Proc. 33rd AAAI Conf. Artif. Intell., 31st Innov. Appl. Artif. Intell. Conf.*, vol. 33, Honolulu, HI, USA. AAAI Press, Jan. 2019, pp. 1409–1416, doi: 10.1609/aaai.v33i01.33011409.

[127] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, and D. Pei, "Robust anomaly detection for multivariate time series through stochastic recurrent neural network," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Anchorage, AK, USA, Jul. 2019, pp. 2828–2837, doi: 10.1145/3292500.3330672.

[128] A. Geiger, D. Liu, S. Alnegheimish, A. Cuesta-Infante, and K. Veeramachaneni, "TadGAN: Time series anomaly detection using generative adversarial networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 33–43.

[129] M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, "DeepAnT: A deep learning approach for unsupervised anomaly detection in time series," *IEEE Access*, vol. 7, pp. 1991–2005, 2019, doi: 10.1109/ACCESS.2018.2886457.

[130] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long short term memory networks for anomaly detection in time series," in *Proc. 23rd Eur. Symp. Artif. Neural Netw. (ESANN)*, Bruges, Belgium, Apr. 2015. [Online]. Available: http://www.elen.ucl.ac.be/Proceedings/esann/esannpdf/es2015-56.pdf

[131] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. Shroff, "LSTM-based encoder–decoder for multi-sensor anomaly detection," 2016, *arXiv:1607.00148*.

[132] M. S. Shahriar, D. Smith, A. Rahman, M. Freeman, J. Hills, R. Rawnsley, D. Henry, and G. Bishop-Hurley, "Detecting heat events in dairy cows using accelerometers and unsupervised learning," *Comput. Electron. Agricult.*, vol. 128, pp. 20–26, Oct. 2016.

[133] L. Bontemps, V. L. Cao, J. McDermott, and N. Le-Khac, "Collective anomaly detection based on long short-term memory recurrent neural networks," in *Proc. 3rd Int. Conf. Future Data Secur. Eng. (FDSE)*, in Lecture Notes in Computer Science, vol. 10018, Can Tho City, Vietnam, T. K. Dang, R. R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, Eds., Nov. 2016, pp. 141–152, doi: 10.1007/978-3-319-48057-2_9.

[134] M. Lichman. (2013). *UCI Machine Learning Repository*. [Online]. Available: http://archive.ics.uci.edu/ml

[135] D. Park, H. Kim, Y. Hoshi, Z. Erickson, A. Kapusta, and C. C. Kemp, "A multimodal execution monitor with anomaly classification for robot-assisted feeding," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Vancouver, BC, Canada, Sep. 2017, pp. 5406–5413, doi: 10.1109/IROS.2017.8206437.

[136] J. Hochenbaum, O. S. Vallis, and A. Kejariwal, "Automatic anomaly detection in the cloud via statistical learning," 2017, *arXiv:1704.07706*.

[137] K. Hundman, V. Constantinou, C. Laporte, I. Colwell, and T. Soderstrom, "Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding," in *Proc. 24th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2018, pp. 387–395, doi: 10.1145/3219819.3219845.

[138] D. Park, Y. Hoshi, and C. C. Kemp, "A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder," *IEEE Robot. Autom. Lett.*, vol. 3, no. 3, pp. 1544–1551, Jul. 2018, doi: 10.1109/LRA.2018.2801475.

[139] H. Lu, Y. Liu, Z. Fei, and C. Guan, "An outlier detection algorithm based on cross-correlation analysis for time series dataset," *IEEE Access*, vol. 6, pp. 53593–53610, 2018, doi: 10.1109/ACCESS.2018.2870151.

[140] T. Kieu, B. Yang, C. Guo, and C. S. Jensen, "Outlier detection for time series with recurrent autoencoder ensembles," in *Proc. 28hth Int. Joint Conf. Artif. Intell.*, Macao, China, Aug. 2019, pp. 2725–2732, doi: 10.24963/ijcai.2019/378.

[141] M. Thill, W. Konen, and T. Bäck, "Online anomaly detection on the Webscope S5 dataset: A comparative study," in *Proc. Evolving Adapt. Intell. Syst. (EAIS)*, May 2017, pp. 1–8.

[142] J. Gao, X. Song, Q. Wen, P. Wang, L. Sun, and H. Xu, "RobustTAD: Robust time series anomaly detection via decomposition and convolutional neural networks," 2020, *arXiv:2002.09545*.

[143] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.

[144] H. Xiao, K. Rasul, and R. Vollgraf, "Fashion-MNIST: A novel image dataset for benchmarking machine learning algorithms," 2017, *arXiv:1708.07747*.

[145] J. J. Hull, "A database for handwritten text recognition research," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 5, pp. 550–554, May 1994, doi: 10.1109/34.291440.

[146] Y. LeCun and C. Cortes. (2010). *MNIST Handwritten Digit Database*. AT&T Labs. [Online]. Available: http://yann.lecun.com/exdb/mnist

[147] A. Krizhevsky and G. Hinton. (2009). *Learning Multiple Layers of Features From Tiny Images*. [Online]. Available: https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf

[148] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VI, USA, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds., Oct. 2007, pp. 366–374, doi: 10.1145/1315245.1315291.

[149] G. Griffin, a. Holub, and P. Perona, "Caltech-256," Caltech Mimeo, Tech. Rep., 2007.

[150] J. Stallkamp, M. Schlipsing, J. Salmen, and C. Igel, "The German traffic sign recognition benchmark: A multi-class classification competition," in *Proc. Int. Joint Conf. Neural Netw.*, San Jose, CA, USA, Jul. 2011, pp. 1453–1460, doi: 10.1109/IJCNN.2011.6033395.

[151] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Salt Lake City, UT, USA, Jun. 2018, pp. 6479–6488. [Online]. Available: http://openaccess.thecvf.com/content

[152] L. Li, W. Huang, I. Y.-H. Gu, and Q. Tian, "Statistical modeling of complex backgrounds for foreground object detection," *IEEE Trans. Image Process.*, vol. 13, no. 11, pp. 1459–1472, Nov. 2004, doi: 10.1109/TIP.2004.836169.

[153] B. Ferrell and S. Santuro. (2005). *Nasa Shuttle Valve Data*. [Online]. Available: http://www.cs.fit.edu/~pkc/nasa/data/

[154] J. J. Van Wijk and E. R. Van Selow, "Cluster and calendar based visualization of time series data," in *Proc. IEEE Symp. Inf. Visualizat. (InfoVis)*, Oct. 1999, pp. 4–9, doi: 10.1109/INFVIS.1999.801851.

[155] L. Ruff, N. Görnitz, L. Deecke, S. A. Siddiqui, R. A. Vandermeulen, A. Binder, E. Müller, and M. Kloft, "Deep one-class classification," in *Proc. 35th Int. Conf. Mach. Learn. (ICML)*, in Proceedings of Machine Learning Research, vol. 80, Stockholm, Sweden, J. G. Dy and A. Krause, Eds., Jul. 2018, pp. 4390–4399. [Online]. Available: http://proceedings.mlr.press/v80/ruff18a.html

[156] L. Xiong, X. Chen, and J. Schneider, "Direct robust matrix factorizatoin for anomaly detection," in *Proc. IEEE 11th Int. Conf. Data Mining*, Vancouver, BC, Canada, Dec. 2011, pp. 844–853, doi: 10.1109/ICDM.2011.52.

[157] D. Velayudhan, T. Hassan, E. Damiani, and N. Werghi, "Recent advances in baggage threat detection: A comprehensive and systematic survey," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–38, Aug. 2023, doi: 10.1145/3549932.

[158] B. Saleh, A. Farhadi, and A. Elgammal, "Object-centric anomaly detection by attribute-based reasoning," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Portland, OR, USA, Jun. 2013, pp. 787–794, doi: 10.1109/CVPR.2013.107.

[159] P. Oza and V. M. Patel, "One-class convolutional neural network," *IEEE Signal Process. Lett.*, vol. 26, no. 2, pp. 277–281, Feb. 2019, doi: 10.1109/LSP.2018.2889273.

[160] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Niagara Falls, NY, USA, Sep. 2016, pp. 1–8, doi: 10.1109/BTAS.2016.7791155.

[161] T. Kieu, B. Yang, and C. S. Jensen, "Outlier detection for multidimensional time series using deep neural networks," in *Proc. 19th IEEE Int. Conf. Mobile Data Manage. (MDM)*, Jun. 2018, pp. 125–134.

[162] H. A. Dau, E. Keogh, K. Kamgar, C.-C. M. Yeh, Y. Zhu, S. Gharghabi, C. A. Ratanamahatana, Yanping, B. Hu, N. Begum, A. Bagnall, A. Mueen, and G. Batista. (2018). *The UCR Time Series Classification Archive*. Hexagon-ML. [Online]. Available: https://www.cs.ucr.edu/ eamonn/timeseriesdata2018/

[163] S. Dagstuhl. (2024). *DBLP Computer Science Bibliography*. Leibniz Center for Informat. University of Trier. [Online]. Available: https://dblp.uni-trier.de

[164] Google Scholar. (2024). *Top Publications*. [Online]. Available: https://scholar.google.com/citations?viewop=topvenues

[165] J. Saives, C. Pianon, and G. Faraut, "Activity discovery and detection of behavioral deviations of an inhabitant from binary sensors," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 4, pp. 1211–1224, Oct. 2015, doi: 10.1109/TASE.2015.2471842.

[166] T. Kleinberger, M. Becker, E. Ras, A. Holzinger, and P. Müller, "Ambient intelligence in assisted living: Enable elderly people to handle future interfaces," in *Proc. 4th Int. Conf. Universal Access Human-Comput. Interact. (UAHCI)*, in Lecture Notes in Computer Science, vol. 4555, Beijing, China, C. Stephanidis, Ed. Springer, Jul. 2007, pp. 103–112, doi: 10.1007/978-3-540-73281-5_11.

[167] A. C. Tran, S. Marsland, J. Dietrich, H. W. Guesgen, and P. Lyons, "Use cases for abnormal behaviour detection in smart homes," in *Proc. 8th Int. Conf. Smart Homes Health Telematics (ICOST)*, in Lecture Notes in Computer Science, vol. 6159, Seoul, South Korea, Y. Lee, Z. Z. Bien, M. Mokhtari, J. T. Kim, M. Park, J. Kim, H. Lee, and I. Khalil, Eds. Springer, 2010, pp. 144–151, doi: 10.1007/978-3-642-13778-5_18.

[168] V. Mirchevska, M. Lustrek, and M. Gams, "Combining domain knowledge and machine learning for robust fall detection," *Expert Syst.*, vol. 31, no. 2, pp. 163–175, May 2014, doi: 10.1111/exsy.12019.

[169] M. Lustrek, H. Gjoreski, N. González Vega, S. Kozina, B. Cvetkovic, V. Mirchevska, and M. Gams, "Fall detection using location sensors and accelerometers," *IEEE Pervasive Comput.*, vol. 14, no. 4, pp. 72–79, Oct. 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7310837/

[170] L. G. Fahad and S. F. Tahir, "Activity recognition and anomaly detection in smart homes," *Neurocomputing*, vol. 423, pp. 362–372, Jan. 2021, doi: 10.1016/j.neucom.2020.10.102.

[171] K. A. Alaghbari, M. H. Md. Saad, A. Hussain, and M. R. Alam, "Activities recognition, anomaly detection and next activity prediction based on neural networks in smart homes," *IEEE Access*, vol. 10, pp. 28219–28232, 2022, doi: 10.1109/ACCESS.2022.3157726.

[172] G. Sprint, D. Cook, R. Fritz, and M. Schmitter-Edgecombe, "Detecting health and behavior change by analyzing smart home sensor data," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, St Louis, MO, USA, May 2016, pp. 1–3, doi: 10.1109/SMARTCOMP.2016.7501687.

[173] J. Dahmen and D. J. Cook, "Indirectly supervised anomaly detection of clinically meaningful health events from smart home data," *ACM Trans. Intell. Syst. Technol.*, vol. 12, no. 2, pp. 1–18, Apr. 2021, doi: 10.1145/3439870.

[174] K. Fouquet, G. Faraut, and J.-J. Lesage, "Model-based approach for anomaly detection in smart home inhabitant daily life," in *Proc. Amer. Control Conf. (ACC)*, New Orleans, LA, USA, May 2021, pp. 3596–3601, doi: 10.23919/ACC50511.2021.9483053.

[175] Z. K. Shahid, S. Saguna, and C. Åhlund, "Unsupervised forecasting and anomaly detection of ADLs in single-resident elderly smart homes," in *Proc. 38th ACM/SIGAPP Symp. Appl. Comput.*, Tallinn, Estonia, Mar. 2023, pp. 607–610, doi: 10.1145/3555776.3577822.

[176] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, "Anomaly detection models for smart home security," in *Proc. IEEE IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, Washington, DC, USA, May 2019, pp. 19–24, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00015.

[177] N. Alsabilah and D. B. Rawat, "Anomaly detection in smart home networks using Kalman filter," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Vancouver, BC, Canada, May 2021, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484507.

[178] X. Li, H. Ghodosi, C. Chen, M. Sankupellay, and I. Lee, "Improving network-based anomaly detection in smart home environment," *Sensors*, vol. 22, no. 15, p. 5626, Jul. 2022, doi: 10.3390/s22155626.

[179] I. Priyadarshini, A. Alkhayyat, A. Gehlot, and R. Kumar, "Time series analysis and anomaly detection for trustworthy smart homes," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108193, doi: 10.1016/j.compeleceng.2022.108193.

[180] Y. Meidan, D. Avraham, H. Libhaber, and A. Shabtai, "CADeSH: Collaborative anomaly detection for smart homes," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8514–8532, May 2023, doi: 10.1109/JIOT.2022.3194813.

[181] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, and K. Saleem, "IoT network anomaly detection in smart homes using machine learning," *IEEE Access*, vol. 11, pp. 119462–119480, 2023, doi: 10.1109/ACCESS.2023.3325929.

[182] S. Munir and J. A. Stankovic, "FailureSense: Detecting sensor failure using electrical appliances in the home," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Philadelphia, PA, USA, Oct. 2014, pp. 73–81, doi: 10.1109/MASS.2014.16.

[183] H. Jung, W. Kim, H. Seo, and Y. Lee, "Simultaneous sporadic sensor anomaly detection for smart homes," in *Proc. 20th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2022, pp. 1061–1066, doi: 10.1145/3560905.3567767.

[184] T. Cultice, D. Ionel, and H. Thapliyal, "Smart home sensor anomaly detection using convolutional autoencoder neural network," in *Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES) (Formerly iNiS)*, Chennai, India, Dec. 2020, pp. 67–70, doi: 10.1109/iSES50453.2020.00026.

[185] C. Fu, Q. Zeng, and X. Du, "Hawatcher: Semantics-aware anomaly detection for Appified smart homes," in *Proc. 30th USENIX Security Symp.*, M. D. Bailey and R. Greenstadt, Eds. USENIX Association, Aug. 2021, pp. 4223–4240. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong

[186] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection in smart home operation from user behaviors and home conditions," *IEEE Trans. Consum. Electron.*, vol. 66, no. 2, pp. 183–192, May 2020, doi: 10.1109/TCE.2020.2981636.

[187] A. Mirugwe, "Accurate occupancy detection of an office room from light, temperature, humidity and CO_2 measurements using statistical learning models," *SSRN Electron. J.*, vol. 112, pp. 28–39, Jan. 2016.

[188] C.-L. Liu, W.-H. Hsaio, and Y.-C. Tu, "Time series classification with multivariate convolutional neural network," *IEEE Trans. Ind. Electron.*, vol. 66, no. 6, pp. 4788–4797, Jun. 2019, doi: 10.1109/TIE.2018.2864702.

[189] T. W. Hnat, V. Srinivasan, J. Lu, T. I. Sookoor, R. Dawson, J. Stankovic, and K. Whitehouse, "The hitchhiker's guide to successful residential sensing deployments," in *Proc. 9th ACM Conf. Embedded Networked Sensor Syst.*, Seattle, WA, USA, Nov. 2011, pp. 232–245, doi: 10.1145/2070942.2070966.

[190] B. Kaluza, V. Mirchevska, E. Dovgan, M. Lustrek, and M. Gams, "An agent-based approach to care in independent living," in *Proc. 1st Int. Joint Conf. Ambient Intell. (AML)*, in Lecture Notes in Computer Science, vol. 6439, Malaga, Spain, B. E. R. de Ruyter, R. Wichert, D. V. Keyson, P. Markopoulos, N. A. Streitz, M. Divitini, N. Georgantas, and A. M. Gómez, Eds. Berlin, Germany: Springer, Nov. 2010, pp. 177–186, doi: 10.1007/978-3-642-16917-5_18.

[191] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "CASAS: A smart home in a box," *Computer*, vol. 46, no. 7, pp. 62–69, Jul. 2013, doi: 10.1109/MC.2012.328.

[192] A. O. Hoori and Y. Motai, "Multicolumn RBF network," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 4, pp. 766–778, Apr. 2018, doi: 10.1109/TNNLS.2017.2650865.

[193] S. Tang, Z. Gu, Q. Yang, and S. Fu, "Smart home IoT anomaly detection based on ensemble model learning from heterogeneous data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Los Angeles, CA, USA, Dec. 2019, pp. 4185–4190, doi: 10.1109/BigData47090.2019.9006249.

[194] Y. Meidan, D. Avraham, H. Libhaber, and A. Shabtai, Apr. 2022, "CADeSH dataset: Collaborative anomaly detection for smart homes," *Zenodo*, doi: 10.5281/zenodo.6406052.

[195] M. Lustrek, H. Gjoreski, S. Kozina, B. Cvetkovic, V. Mirchevska, and M. Gams, "Detecting falls with location sensors and accelerometers," in *Proc. 23rd Conf. Innov. Appl. Artif. Intell.*, San Francisco, CA, USA, D. G. Shapiro and M. P. J. Fromherz, Eds., Aug. 2011. [Online]. Available: http://www.aaai.org/ocs/index.php/IAAI/IAAI-11/paper/view/2753

[196] D. Fährmann, F. Boutros, P. Kubon, F. Kirchbuchner, A. Kuijper, and N. Damer, "Ubiquitous multi-occupant detection in smart environments," *Neural Comput. Appl.*, vol. 36, no. 6, pp. 2941–2960, Feb. 2024.

[197] T. van Kasteren, A. Noulas, G. Englebienne, and B. Kröse, "Accurate activity recognition in a home setting," in *Proc. 10th Int. Conf. Ubiquitous Comput.*. New York, NY, USA: Association for Computing Machinery, Sep. 2008, pp. 1–9, doi: 10.1145/1409635.1409637.

[198] S. Makonin, 2015, "ODDs: Occupancy detection dataset," *Harvard Dataverse*, doi: 10.7910/DVN/2K9FFE.

[199] G. Michael Youngblood and D. J. Cook, "Data mining for hierarchical model creation," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 4, pp. 561–572, Jul. 2007, doi: 10.1109/TSMCC.2007.897341.

[200] M. Novák, M. Binas, and F. Jakab, "Unobtrusive anomaly detection in presence of elderly in a smart-home environment," in *Proc. ELEKTRO*, May 2012, pp. 341–344.

[201] Y. Djenouri, A. Belhadi, J. C. Lin, D. Djenouri, and A. Cano, "A survey on urban traffic anomalies detection algorithms," *IEEE Access*, vol. 7, pp. 12192–12205, 2019, doi: 10.1109/ACCESS.2019.2893124.

[202] S. Yang and W. Zhou, "Anomaly detection on collective moving patterns: Manifold learning based analysis of traffic streams," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust IEEE 3rd Int. Conf. Social Comput.*, Boston, MA, USA, Oct. 2011, pp. 704–707, doi: 10.1109/PASSAT/SOCIALCOM.2011.10.

[203] S. Chawla, Y. Zheng, and J. Hu, "Inferring the root cause in road traffic anomalies," in *Proc. IEEE 12th Int. Conf. Data Mining*, Brussels, Belgium, Dec. 2012, pp. 141–150, doi: 10.1109/ICDM.2012.104.

[204] L. X. Pang, S. Chawla, W. Liu, and Y. Zheng, "On detection of emerging anomalous traffic patterns using GPS data," *Data Knowl. Eng.*, vol. 87, pp. 357–373, Sep. 2013, doi: 10.1016/j.datak.2013.05.002.

[205] Q. Wang, W. Lv, and B. Du, "Spatio-temporal anomaly detection in traffic data," in *Proc. 2nd Int. Symp. Comput. Sci. Intell. Control*. New York, NY, USA: Association for Computing Machinery, Sep. 2018, pp. 1–5, doi: 10.1145/3284557.3284725.

[206] U. Kaytaz, F. Sivrikaya, and S. Albayrak, "Competitive learning for unsupervised anomaly detection in intelligent transportation systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2022, pp. 5433–5438, doi: 10.1109/ICC45855.2022.9838636.

[207] X. Peng, Y. Lin, Q. Cao, Y. Cen, H. Zhuang, and Z. Lin, "Traffic anomaly detection in intelligent transport applications with time series data using informer," in *Proc. IEEE 25th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2022, pp. 3309–3314, doi: 10.1109/ITSC55140.2022.9922142.

[208] Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, "A taxi driving fraud detection system," in *Proc. IEEE 11th Int. Conf. Data Mining*, Vancouver, BC, Canada, Dec. 2011, pp. 181–190, doi: 10.1109/ICDM.2011.18.

[209] D. Zhang, N. Li, Z.-H. Zhou, C. Chen, L. Sun, and S. Li, "IBAT: Detecting anomalous taxi trajectories from GPS traces," in *Proc. 13th Int. Conf. Ubiquitous Comput.*, Beijing, China, Sep. 2011, pp. 99–108, doi: 10.1145/2030112.2030127.

[210] C. Chen, D. Zhang, P. S. Castro, N. Li, L. Sun, S. Li, and Z. Wang, "IBOAT: Isolation-based online anomalous trajectory detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 806–818, Jun. 2013, doi: 10.1109/TITS.2013.2238531.

[211] A. Belhadi, Y. Djenouri, G. Srivastava, D. Djenouri, A. Cano, and J. C. Lin, "A two-phase anomaly detection model for secure intelligent transportation ride-hailing trajectories," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4496–4506, Jul. 2021, doi: 10.1109/TITS.2020.3022612.

[212] J. Zhang, "Smarter outlier detection and deeper understanding of large-scale taxi trip records: A case study of NYC," in *Proc. ACM SIGKDD Int. Workshop Urban Comput.*, Beijing, China, Aug. 12, 2012, pp. 157–162, doi: 10.1145/2346496.2346521.

[213] F. Seraj, B. J. van der Zwaag, A. Dilo, T. Luarasi, and P. J. M. Havinga, "Roads: A road pavement monitoring system for anomaly detection using smart phones," in *Proc. 5th Int. Workshop Model. Social Media (MSM)*, in Lecture Notes in Computer Science, vol. 9546, M. Atzmueller, A. Chin, F. Janssen, I. Schweizer, and C. Trattner, Eds. Springer, 2014, pp. 128–146, doi: 10.1007/978-3-319-29009-6_7.

[214] A. Witayangkurn, T. Horanont, Y. Sekimoto, and R. Shibasaki, "Anomalous event detection on large-scale GPS data from mobile phones using hidden Markov model and cloud platform," in *Proc. ACM Conf. Pervasive Ubiquitous Comput. Adjunct Publication*, Zurich, Switzerland, Sep. 2013, pp. 1219–1228, doi: 10.1145/2494091.2497352.

[215] X. Kong, H. Gao, O. Alfarraj, Q. Ni, C. Zheng, and G. Shen, "HUAD: Hierarchical urban anomaly detection based on spatio-temporal data," *IEEE Access*, vol. 8, pp. 26573–26582, 2020, doi: 10.1109/ACCESS.2020.2971341.

[216] M. Wilbur, A. Dubey, B. Leão, and S. Bhattacharjee, "A decentralized approach for real time anomaly detection in transportation networks," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Washington, DC, USA, Jun. 2019, pp. 274–282, doi: 10.1109/SMARTCOMP.2019.00063.

[217] R. Wang, F. Kong, H. Sudler, and X. Jiao, "Brief industry paper: HDAD: Hyperdimensional computing-based anomaly detection for automotive sensor attacks," in *Proc. IEEE 27th Real-Time Embedded Technol. Appl. Symp. (RTAS)*, Nashville, TN, USA, May 2021, pp. 461–464, doi: 10.1109/RTAS52030.2021.00052.

[218] V. P. K. Madhavarapu, P. Roy, S. Bhattacharjee, and S. K. Das, "Active learning augmented folded Gaussian model for anomaly detection in smart transportation," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 2762–2767, doi: 10.1109/ICC45855.2022.9838276.

[219] W. Bouzeraib, A. Ghenai, and N. Zeghib, "A multi-objective genetic GAN oversampling: Application to intelligent transport anomaly detection," in *Proc. IEEE 22nd Int. Conf. High Perform. Comput. Commun.; IEEE 18th Int. Conf. Smart City; IEEE 6th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Yanuca Island, Cuvu, Fiji, Dec. 2020, pp. 1142–1149, doi: 10.1109/hpcc-smartcity-dss50907.2020.00148.

[220] P. Mignone, D. Malerba, and M. Ceci, "Anomaly detection for public transport and air pollution analysis," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Osaka, Japan, Dec. 2022, pp. 2867–2874, doi: 10.1109/BigData55660.2022.10020470.

[221] C. Zhao, X. Chang, T. Xie, H. Fujita, and J. Wu, "Unsupervised anomaly detection based method of risk evaluation for road traffic accident," *Int. J. Speech Technol.*, vol. 53, no. 1, pp. 369–384, Jan. 2023, doi: 10.1007/s10489-022-03501-8.

[222] J. Islam, J. P. Talusan, S. Bhattacharjee, F. Tiausas, S. M. Vazirizade, A. Dubey, K. Yasumoto, and S. K. Das, "Anomaly based incident detection in large scale smart transportation systems," in *Proc. ACM/IEEE 13th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Milano, Italy, May 2022, pp. 215–224, doi: 10.1109/ICCPS54341.2022.00026.

[223] Y. Wang, J. Xu, M. Xu, N. Zheng, J. Jiang, and K. Kong, "A feature-based method for traffic anomaly detection," in *Proc. 2nd ACM SIGSPATIAL Workshop Smart Cities Urban Anal.*, Burlingame, CA, USA, H. T. Vo, Ed., Oct. 2016, pp. 5:1–5:8, doi: 10.1145/3007540.3007545.

[224] H. Wu, W. Sun, and B. Zheng, "A fast trajectory outlier detection approach via driving behavior modeling," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Singapore, E. Lim, M. Winslett, M. Sanderson, A. W. Fu, J. Sun, J. S. Culpepper, E. Lo, J. C. Ho, D. Donato, R. Agrawal, Y. Zheng, C. Castillo, A. Sun, V. S. Tseng, and C. Li, Eds., Nov. 2017, pp. 837–846, doi: 10.1145/3132847.3132933.

[225] Y. Zheng, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Smart car parking: Temporal clustering and anomaly detection in urban car parking," in *Proc. IEEE 9th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Singapore, Apr. 2014, pp. 1–6, doi: 10.1109/ISSNIP.2014.6827618.

[226] C. Huang, X. Wu, and D. Wang, "Crowdsourcing-based urban anomaly prediction system for smart cities," in *Proc. 25th ACM Int. Conf. Inf. Knowl. Manage.*, S. Mukhopadhyay, C. Zhai, E. Bertino, F. Crestani, J. Mostafa, J. Tang, L. Si, X. Zhou, Y. Chang, Y. Li, and P. Sondhi, Eds., Oct. 2016, pp. 1969–1972, doi: 10.1145/2983323.2983886.

[227] Y.-C. Tai, C.-W. Chan, and J. Y.-J. Hsu, "Automatic road anomaly detection using smart mobile device," in *Proc. Conf. Technol. Appl. Artif. Intell. (TAAI)*, 2010.

[228] K. Bhowmick and M. Narvekar, "Trajectory outlier detection for traffic events: A survey," in *Intelligent Computing and Information and Communication*, S. Bhalla, V. Bhateja, A. A. Chandavale, A. S. Hiwale, and S. C. Satapathy, Eds. Singapore: Springer, 1007, pp. 37–46.

[229] N. Taxi. (Aug. 2020). *TLC Trip Record Data*. [Online]. Available: https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page

[230] L. Moreira-Matias, M. Ferreira, and J. Mendes-Moreira, "Taxi service trajectory—Prediction challenge, ECML PKDD 2015," UCI Mach. Learn. Repository, Rep., 2015, doi: 10.24432/C55W25.

[231] E. Romera, L. M. Bergasa, and R. Arroyo, "Need data for driver behaviour analysis? Presenting the public UAH-DriveSet," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 387–392.

[232] W. Underground. (Dec. 2020). *Local Weather Forecast*. [Online]. Available: https://www.wunderground.com/

[233] *Here API*. Accessed: Nov. 19, 2023. [Online]. Available: https://developer.here.com/

[234] M. H. Hassan, A. Tizghadam, and A. Leon-Garcia, "Spatio-temporal anomaly detection in intelligent transportation systems," in *Proc. 10th Int. Conf. Ambient Syst., Netw. Technol. (ANT), 2nd Int. Conf. Emerg. Data Ind. 4.0 (EDI40)*, in Procedia Computer Science, vol. 151, Leuven, Belgium, E. M. Shakshuki and A. Yasar, Eds. Amsterdam, The Netherlands: Elsevier, Apr. 2019, pp. 852–857, doi: 10.1016/j.procs.2019.04.117.

[235] C. Kaiser, A. Stocker, and A. Festl, 2019, "Automotive can bus data: An example dataset from the aegis big data project," *Zenodo*, doi: 10.5281/zenodo.3267183.

[236] *Skoltech Anomaly Benchmark (SKAB)*. Accessed: Nov. 19, 2023. [Online]. Available: https://www.kaggle.com/datasets/yuriykatser/skoltech-anomaly-benchmark-skab

[237] (Oct. 2011). *311 Service Requests From 2010 to Present*. [Online]. Available: https://data.cityofnewyork.us/Social-Services/311-Service-Requests-from-2010-to-Present/erm2-nwe9

[238] Lyft. (2022). *CitiBike*. Accessed: Sep. 27, 2022. [Online]. Available: https://ride.citibikenyc.com/system-data

[239] E. Hozdić, "Smart factory for Industry 4.0: A review," *Int. J. Mod. Manuf. Technol.*, vol. 7, no. 1, pp. 28–35, 2015.

[240] M. Mabkhot, A. Al-Ahmari, B. Salah, and H. Alkhalefah, "Requirements of the smart factory system: A survey and perspective," *Machines*, vol. 6, no. 2, p. 23, Jun. 2018. [Online]. Available: https://www.mdpi.com/2075-1702/6/2/23

[241] (2010). *Cyber-Physical Systems (CPS)*. [Online]. Available: https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

[242] J. Ding, Y. Atif, S. F. Andler, B. Lindström, and M. Jeusfeld, "CPS-based threat modeling for critical infrastructure protection," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 45, no. 2, pp. 129–132, Oct. 2017, doi: 10.1145/3152042.3152080.

[243] Government of Federal Ministry of Education and Research. (Aug. 2020). *What is Industrie 4.0?*. [Online]. Available: https://www.plattform-i40.de/PI40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html

[244] Government of Federal Ministry of Economic Affairs and Energy. (Aug. 2019). *2030 Vision for Industrie 4.0*. [Online]. Available: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Positionspapier

[245] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, Selangor Darul Ehsan, Malaysia, Dec. 2014, pp. 697–701, doi: 10.1109/IEEM.2014.7058728.

[246] Y. Zhang, P. Peng, C. Liu, and H. Zhang, "Anomaly detection for industry product quality inspection based on Gaussian restricted Boltzmann machine," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Bari, Italy, Oct. 2019, pp. 1–6, doi: 10.1109/SMC.2019.8914524.

[247] Q. Tang and H. Jung, "Reliable anomaly detection and localization system: Implications on manufacturing industry," *IEEE Access*, vol. 11, pp. 114613–114622, 2023, doi: 10.1109/ACCESS.2023.3324314.

[248] T. Arndt, M. Conzen, I. Elsen, A. Ferrein, O. Galla, H. KöSe, S. Schiffer, and M. Tschesche, "Anomaly detection in the metal-textile industry for the reduction of the cognitive load of quality control workers," in *Proc. 16th Int. Conf. Pervasive Technol. Rel. Assistive Environments*, Corfu, Greece, Jul. 2023, pp. 535–542, doi: 10.1145/3594806.3596558.

[249] M. Carletti, C. Masiero, A. Beghi, and G. A. Susto, "Explainable machine learning in Industry 4.0: Evaluating feature importance in anomaly detection to enable root cause analysis," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Bari, Bari, Italy, Oct. 2019, pp. 21–26, doi: 10.1109/SMC.2019.8913901.

[250] Y. Liu, X. Gao, J. Z. Wen, and H. Luo, "Unsupervised image anomaly detection and localization in industry based on self-updated memory and center clustering," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–10, 2023, doi: 10.1109/TIM.2023.3271754.

[251] A. Acernese, K. Sarda, V. Nolè, L. Manfredi, L. Greco, L. Glielmo, and C. Del Vecchio, "Robust statistics-based anomaly detection in a steel industry," in *Proc. 29th Medit. Conf. Control Autom. (MED)*, Bari, Italy, Jun. 2021, pp. 1058–1063, doi: 10.1109/MED51440.2021.9480311.

[252] K. Sarda, A. Acernese, V. Nolè, L. Manfredi, L. Greco, L. Glielmo, and C. D. Vecchio, "A multi-step anomaly detection strategy based on robust distances for the steel industry," *IEEE Access*, vol. 9, pp. 53827–53837, 2021, doi: 10.1109/ACCESS.2021.3070659.

[253] P. Tanuska, L. Spendla, M. Kebisek, R. Duris, and M. Stremy, "Smart anomaly detection and prediction for assembly process maintenance in compliance with Industry 4.0," *Sensors*, vol. 21, no. 7, p. 2376, Mar. 2021, doi: 10.3390/s21072376.

[254] A. Rodriguez, D. Bourne, M. T. Mason, G. F. Rossano, and J. Wang, "Failure detection in assembly: Force signature analysis," in *Proc. IEEE Conf. Autom. Sci. Eng. (CASE)*, Toronto, ON, Canada, Aug. 2010, pp. 210–215, doi: 10.1109/COASE.2010.5584452.

[255] N. Davari, B. Veloso, R. P. Ribeiro, P. M. Pereira, and J. Gama, "Predictive maintenance based on anomaly detection using deep learning for air production unit in the railway industry," in *Proc. IEEE 8th Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Porto, Portugal, Oct. 2021, pp. 1–10, doi: 10.1109/DSAA53316.2021.9564181.

[256] D. Velásquez, E. Pérez, X. Oregui, A. Artetxe, J. Manteca, J. E. Mansilla, M. Toro, M. Maiza, and B. Sierra, "A hybrid machine-learning ensemble for anomaly detection in real-time Industry 4.0 systems," *IEEE Access*, vol. 10, pp. 72024–72036, 2022, doi: 10.1109/ACCESS.2022.3188102.

[257] G. P. Tancredi, G. Vignali, and E. Bottani, "Integration of digital twin, machine-learning and Industry 4.0 tools for anomaly detection: An application to a food plant," *Sensors*, vol. 22, no. 11, p. 4143, May 2022, doi: 10.3390/s22114143.

[258] B. Lindemann, F. Fesenmayr, N. Jazdi, and M. Weyrich, "Anomaly detection in discrete manufacturing using self-learning approaches," *Proc. CIRP*, vol. 79, pp. 313–318, Jan. 2019, doi: 10.1016/j.procir.2019.02.073.

[259] A. E. Kalør, D. Michelsanti, F. Chiariotti, Z.-H. Tan, and P. Popovski, "Remote anomaly detection in Industry 4.0 using resource-constrained devices," in *Proc. IEEE 22nd Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Lucca, Italy, Sep. 2021, pp. 251–255, doi: 10.1109/SPAWC51858.2021.9593188.

[260] K. Demertzis, L. Iliadis, N. Tziritas, and P. Kikiras, "Anomaly detection via blockchained deep learning smart contracts in Industry 4.0," *Neural Comput. Appl.*, vol. 32, no. 23, pp. 17361–17378, Dec. 2020, doi: 10.1007/s00521-020-05189-8.

[261] L. Qi, Y. Yang, X. Zhou, W. Rafique, and J. Ma, "Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure Industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6503–6511, Sep. 2022, doi: 10.1109/TII.2021.3139363.

[262] F. Jin, H. Wu, Y. Liu, J. Zhao, and W. Wang, "Varying-scale HCA-DBSCAN-based anomaly detection method for multi-dimensional energy data in steel industry," *Inf. Sci.*, vol. 647, Nov. 2023, Art. no. 119479, doi: 10.1016/j.ins.2023.119479.

[263] D. Fährmann, N. Damer, F. Kirchbuchner, and A. Kuijper, "Lightweight long short-term memory variational auto-encoder for multivariate time series anomaly detection in industrial control systems," *Sensors*, vol. 22, no. 8, p. 2886, Apr. 2022, doi: 10.3390/s22082886.

[264] T. Tagaris, G. Ioannou, M. Sdraka, G. Alexandridis, and A. Stafylopatis, "Putting together wavelet-based scaleograms and convolutional neural networks for anomaly detection in nuclear reactors," in *Proc. 3rd Int. Conf. Adv. Artif. Intell.*, Istanbul, Turkey, Oct. 2019, pp. 237–243, doi: 10.1145/3369114.3369121.

[265] F. Calivá, F. S. De Ribeiro, A. Mylonakis, C. Demazi'ere, P. Vinai, G. Leontidis, and S. Kollias, "A deep learning approach to anomaly detection in nuclear reactors," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Rio de Janeiro, Brazil, Jul. 2018, pp. 1–8, doi: 10.1109/IJCNN.2018.8489130.

[266] C. Demazière, "CORE SIM: A multi-purpose neutronic tool for research and education," *Ann. Nucl. Energy*, vol. 38, no. 12, pp. 2698–2718, Dec. 2011. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0306454911002210

[267] P. Cortez, A. Cerdeira, F. Almeida, T. Matos, and J. Reis, "Modeling wine preferences by data mining from physicochemical properties," *Decis. Support Syst.*, vol. 47, no. 4, pp. 547–553, Nov. 2009, doi: 10.1016/j.dss.2009.05.016.

[268] N. Wang, Z. Zhang, X. Zhao, Q. Miao, R. Ji, and Y. Gao, "Exploring high-order correlations for industry anomaly detection," *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9682–9691, Dec. 2019, doi: 10.1109/TIE.2019.2907441.

[269] H. Purohit, R. Tanabe, T. Ichige, T. Endo, Y. Nikaido, K. Suefusa, and Y. Kawaguchi, "MIMII dataset: Sound dataset for malfunctioning industrial machine investigation and inspection," in *Proc. Detection Classification Acoustic Scenes Events Workshop (DCASE)*, M. I. Mandel, J. Salamon, and D. P. W. Ellis, Eds. New York, NY, USA: New York University, Oct. 2019, pp. 209–213. [Online]. Available: http://dcase.community/documents/workshop2019/proceedings/DCASE2019Workshop

[270] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6, doi: 10.1109/MILCIS.2015.7348942.

[271] P. Bergmann, M. Fauser, D. Sattlegger, and C. Steger, "MVTec AD—A comprehensive real-world dataset for unsupervised anomaly detection," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Long Beach, CA, USA, Jun. 2019, pp. 9584–9592.

[272] Á. L. P. Gómez, L. F. Maimó, A. H. Celdrán, F. J. G. Clemente, C. C. Sarmiento, C. J. D. C. Masa, and R. M. Nistal, "On the generation of anomaly detection datasets in industrial control systems," *IEEE Access*, vol. 7, pp. 177460–177473, 2019, doi: 10.1109/ACCESS.2019.2958284.

[273] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "WADI: A water distribution testbed for research in the design of secure cyber physical systems," in *Proc. 3rd Int. Workshop Cyber-Phys. Syst. Smart Water Netw.*, Pittsburgh, PA, USA, Apr. 2017, pp. 25–28, doi: 10.1145/3055366.3055375.

[274] R. Taormina and S. Galelli, "Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems," *J. Water Resour. Planning Manage.*, vol. 144, no. 10, Oct. 2018, Art. no. 04018065.

[275] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, "A control system testbed to validate critical infrastructure protection concepts," *Int. J. Crit. Infrastruct. Protection*, vol. 4, no. 2, pp. 88–103, Aug. 2011, doi: 10.1016/j.ijcip.2011.06.005.

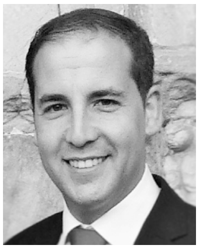
[276] A. P. Mathur and N. O. Tippenhauer, "SWaT: A water treatment testbed for research and training on ICS security," in *Proc. Int. Workshop Cyber-Phys. Syst. Smart Water Netw. (CySWater)*, Vienna, Austria, Apr. 2016, pp. 31–36, doi: 10.1109/CYSWATER.2016.7469060.

[277] iTrust. *Centre for Research in Cyber Security*. Accessed: Jan. 6, 2022. [Online]. Available: https://itrust.sutd.edu.sg

[278] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Proc. Int. Conf. Crit. Inf. Infrastruct. Secur.*, in Lecture Notes in Computer Science, Paris, France, G. M. Havârneanu, R. Setola, H. Nassopoulos, and S. D. Wolthusen, Eds. Switzerland: Springer, Oct. 2016, pp. 88–99, doi: 10.1007/978-3-319-71368-7_8.

DANIEL FÄHRMANN received the Bachelor of Science degree in applied computer science from Baden-Württemberg Cooperative State University, in 2013, and the Master of Science degree in computer science from Darmstadt University of Technology, in 2019. During the bachelor's degree, the Hewlett-Packard GmbH employed him as part of his dual study program. From 2012 to 2015, he continued his work at HP, as an IT Consultant for VoIP and network technologies. From 2016 to 2020, he was a Research Assistant with the Smart Living and Biometric Technologies Department, Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, where he has been a Research Associate, since February 2020. His research interests include situation recognition in smart environments, anomaly detection, and safe and secure smart cities.

LAURA MARTÍN received the master's degree in telecommunications engineering from Universidad de Cantabria, in 2022, where she is currently pursuing the Ph.D. degree in telecommunications engineering. She is a Research Fellow with the Network Planning and Mobile Communications Laboratory, Universidad de Cantabria, Spain. Her research interests include the application of artificial intelligence for the enrichment of the IoT data. Moreover, she is also active on applying semantic web principles to data sharing and, this way, developing a fully distributed enriched data sharing ecosystem.



LUIS SÁNCHEZ received the M.Sc. and Ph.D. degrees in telecommunications engineering, in 2002 and 2009, respectively. He is currently an Associate Professor with Universidad de Cantabria, Spain. He is active on the IoT-enabled smart cities and the application of AI for data enrichment. He has led and/or participated in more than 15 projects belonging to different EU framework programs. He has authored more than 60 papers at international journals and conferences. He often participates in panels discussing about innovation supported by the IoT in smart cities. He also acts as an expert for several European countries national funding agencies.

NASER DAMER (Senior Member, IEEE) received the Ph.D. degree in computer science from TU Darmstadt, in 2018. He is currently a Senior Researcher with Fraunhofer IGD, performing research management, applied research, scientific consulting, and system evaluation. He is the Principal Investigator of the National Research Center for Applied Cybersecurity ATHENE, Germany. He lectures on human and identity-centric machine learning and ambient intelligence with TU Darmstadt. His research interests include the fields of biometrics, machine learning, and information fusion. He is a member of the organizing teams of several conferences, workshops, and special sessions, including being the Program Co-Chair of BIOSIG. He is a member of the IEEE Biometrics Council serving on its Technical Activities Committee. He represents German Institute for Standardization (DIN) in the ISO/IEC SC37 International Biometrics Standardization Committee. He serves as an Associate Editor for *Pattern Recognition* (Elsevier) and *The Visual Computer* (Springer).