IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 September 2022, accepted 15 October 2022, date of publication 19 October 2022, date of current version 31 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3216007

PERSPECTIVE

A Review of Neural Networks for Anomaly Detection

JOSÉ EDSON DE ALBUQUERQUE FILHO, LAISLLA C. P. BRANDÃO, BRUNO JOSÉ TORRES FERNANDES, (Senior Member, IEEE), AND ALEXANDRE M. A. MACIEL

Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife 50720-001, Brazil

Corresponding author: José Edson De Albuquerque Filho (jeaf@ecomp.poli.br)

This work was supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

ABSTRACT Anomaly detection is a critical issue across several academic fields and real-world applications. Artificial neural networks have been proposed to detect anomalies from different input types, but there is no clear guide to deciding which model to use in a specific case. Therefore, this study examines the most relevant Neural Network Outlier Detection algorithms in the literature, compares their benefits and drawbacks in some application scenarios, and displays their outcomes in benchmark datasets. The initial search revealed 1422 papers on projects completed between 2017 and 2021. These papers were further narrowed based on title, abstract, quality assessment, inclusion, and exclusion criteria, remaining 76 articles. Finally, we reviewed these publications and verified that Autoencoder Neural Network, Convolutional Neural Network, Recurrent Neural Network, and Generative Adversarial Network have promisor outcomes for outlier detection, the advantages of these neural networks for outlier detection, and the significant challenges of outlier detection strategies.

INDEX TERMS Anomaly detection, neural networks, outlier detection, systematic review.

I. INTRODUCTION

In data mining, anomaly detection or (outliers detecion) means identifying arouse suspicion samples because they differ significantly from most data, as shown in the Figure 1.

It is not easy to solve the problem of detecting anomalies in a wide sense.The majority of known anomaly detection approaches address a specific problem formulation. Several aspects influence the formulation, including the nature of the data, the availability of known anomalies in the training data, the sort of abnormalities to be found, and so on. The application domain in which the anomaly must be discovered determines these characteristics usually. Researchers have adopted concepts from various disciplines, such as statistics, machine learning, computational intelligence, data mining, and information theory, among others, and applied them in formulating specific cases.

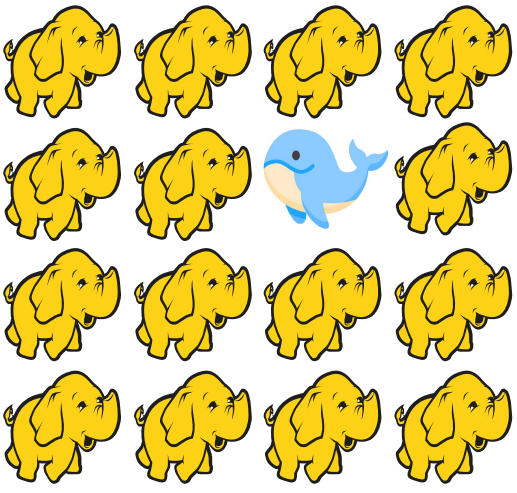


FIGURE 1. A whale is an anomaly in a herd of elephants.

Several factors make this seemingly simple problem complex: defining an embracing edge of all normal behavior is very hard because the boundary between ordinary and

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

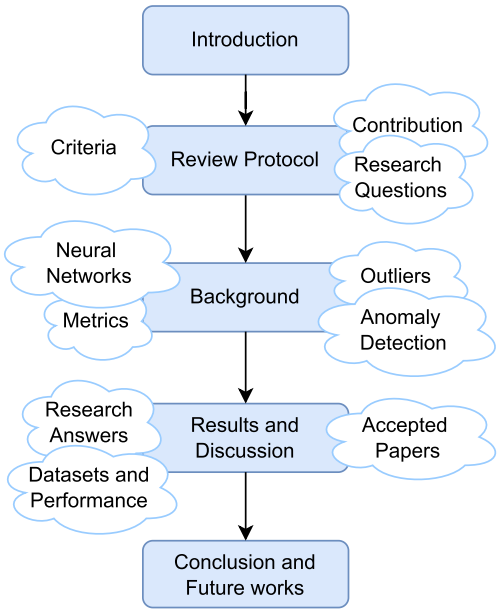


FIGURE 2. This diagram illustrates the structure of this review.

anomalous behavior is blurred and unclear. For that reason, an anomalous instance that approaches the limit might be considered normal, and vice versa.

When anomalies results from malicious actions, the action creators try to make the anomalous observations look normal, making the mission of defining normal behavior even more difficult. In many domains the normal behavior continues to evolve and a notion of what normal behavior would be in the present may not be representative in the future [1].

An outlier is differently defined according to the application-specific domain. For example, a tiny variation from standard, such as a changing body temperature, can be deemed an anomaly in the medical sector. On the other hand, a similar deviation in the stock market can be considered typical. As a result, transferring a technique created for one domain to another is not straightforward.

Usually the availability of sets of data with anomalies necessary for training and validation of detection models is small, which makes it more complex to define the abnormal behavior. Furthermore, data often include noise that are close to true anomalies, making it difficult to recognize and delete them.

Neural networks stand out compared to classical approaches in context with complex behavioral or time-varying data. For this reason, the main objective of this study is to conduct a review of the embracing literature on anomaly detection and its applications using neural networks. Thereby, readers will have a better understanding of the different detection techniques involving neural networks.

The structure of this review has five sections: Introduction, Review Protocol, Background, Results and Discussion anf finally Results and Future Works, as shown in Figure 2.

While the latest surveys present general machine learning for anomaly detection, this work differs from them because it presents comprehensive research on anomaly detection through machine learning techniques focusing on neural networks and covering the period from 2017 to 2021

Our review did not identify any other survey covering neural networks for anomaly detection. Therefore, this review differs from the latest surveys because it presents comprehensive research on anomaly detection through machine learning techniques focusing on neural networks and covering the period from 2017 to 2021. This paper's contributions aim to provide a comprehensive review of neural networks for anomaly detection and a guide to deciding which model to use in a specific case.

The remainder of this paper is structured as follows. Section II details this survey protocol and reveals the research questions. Section III introduces some important concepts for a better understanding. Section IV show some related works. Section V presents survey results. Finally, Section VI shows the conclusion and future works.

II. REVIEW PROTOCOL

The focus of this survey is publications of primary research that address issues related to anomaly detection. In addition, the search is for works published in international scientific journals during last five years and that employ machine learning methods and tools for their purposes especially those that use neural networks. This survey follows initial steps from the protocol proposed by Kitchenham [2], [3]. A systematic review of the literature provides a means for evaluating and interpreting available research that is pertinent to a specific subject area.

According to kitchenham [2], the systematic review has three phases: planning, conducting, and reporting the study. This study reflects a very similar structure:

1) Identification of research questions (Section II-B)
2) Development of search parameters and exclusion and inclusion criteria (Section II-C)
3) Search Results (Section V)

For the best didactic purpose, Figure 3 expands the adopted research methodology for this systematic review.

A. CONTRIBUTION

Most of the current literature on anomaly detection is focused on specific applications or a specific area of research [4]. This work contributes with an overview of different research areas and applications. In addition, it highlights the richness and complexity associated with each application domain to guide the decision of which model to use in a specific case.

B. DEFINITION OF RESEARCH QUESTIONS

The aim is to systematically collect, evaluate and interpret all published studies relevant to the predefined research questions in order to provide consolidated information, list the benefits of certain approaches and to find a research gap that can be filled through investigation. [3].

FIGURE 3. Protocol steps.

TABLE 1. Primary query search parameters.

Description	Terms
Application Field	Neural Network
Application Purpose	Outlier Detection OR Anomaly Detection
Time Period	2017-2021
Language	English
Paper Types	Journal and Conference only

Research questions:

1) What kind of Neural Networks are used to outlier detection? (Section V-C)
2) What are Neural Networks strengths for outlier detection? (Section V-D)
3) What are the current challenges of outlier detection techniques? (Section V-E)

C. SEARCH CRITERIA

This study aims to identify relevant articles on anomaly detection using neural networks. Therefore we select primary papers based on keywords, search period and, inclusion and exclusion criteria. The main research keywords included are described below in the Table 1.

The search query was stated by fields and purpose applications and limited to the last 5 years. This work was conducted in the leading digital libraries, as shown in Table 2.

The research exposed a large volume of literature, including journal publications, conference annals and many other published materials as shown in Table 5. All digital repositories included were manually searched using predefined keywords with some synonyms, according criteria in Table 3 and quality assessment in Table 4.

TABLE 2. Selected review sources.

Publisher	URL
IEEE Xplore	ieeexplore.ieee.org
ACM Digital Library	www.dl.acm.org
Web Of Science	www.webofscience.com
SCOPUS	www.scopus.com
Science Direct	www.sciencedirect.com

TABLE 3. List of all inclusion and exclusion criteria.

Inclusion criteria
1) Compare neural network outlier detectors.
2) Use neural networks for outlier detection.
3) Only journal and Conference paper.
4) Published in Time
Exlusion Criteria
1) Approach only for specific purpose.
2) Paper is not available online.
3) Poster, tutorial, editorial, short paper.
4) Unfinished works.
5) Paper not in English language.
6) Do not match an inclusion criterion.

D. QUALITY ASSESSMENT

To assess the compliance of the papers with the research questions, a questionnaire with eight questions was applied. There are three possible answers: Yes (Y), Partially (P) and No (N) with specific weights for each question.

TABLE 4. Quality assessment rules.

ID	Quality Criteria	Answers
QC1	Is there a model implementation description?	(Y) = 1.0; (P) = 0.5; (N) = 0
QC2	Does the paper expose method strengths?	(Y) = 2.0; (P) = 1.0; (N) = 0
QC3	Does the study expose method limitations?	(Y) = 3.0; (P) = 1.0; (N) = 0
QC4	Are the results reported clearly?	(Y) = 1.0; (P) = 0.5; (N) = 0
QC5	Are the future works and contributions clearly described?	(Y) = 2.0; (P) = 1.0; (N) = 0
QC6	Does the paper shows some reseach gap?	(Y) = 4.0; (P) = 2.0; (N) = 0

III. BACKGROUND

In this section, we will define some important concepts for a better understanding of the article, highlighting the concepts of anomalies and neural networks.

A. OUTLIERS

From the beginning of the research, we encountered several definitions of what an anomaly (outlier) would be. Here are some of them:

- Because the stochastic model does not create it, an outlier is thought to be partially or wholly unimportant [5].
- An outlier, or external observation, seems to diverge significantly from the other group members in which it originates [6].
- An outlier is an observation that differs so significantly from the rest of the data that it raises concerns that it was generated by a distinct process [7].
- An observation (or selection of observations) looks out of place in this dataset [8].
- Outliers are points with lower local density in comparison with the density of their neighborhood [9].
- Outliers are points that do not belong to the dataset or are subgroups that are considerably smaller than other subgroups [10].
- Outliers instances are not well generated in the output layer and have a significant reconstruction error [11].
- If the region's density where the data instance is located is considerably less or greater than the neighboring clusters, they are termed outliers [12].
- A point is considered an outlier if in some projection of a smaller dimension it is present in a local region of very low density [13].
- An outlier is a data that is very different from the others, or that does not conform to expected normal behavior, or that conforms to defined abnormal behavior [14].

This demonstrates how complex it is to provide a precise definition of what an outlier is. In this work, we will use a broader definition: anomalies are those exceptional data that deviate from the general pattern.

It is also necessary to consider some inherent factors to understand the anomalies that may indicate error, failure, fraud or intrusion. For instance, noise promotes a change in the value of a data regarding its value without noise, it has no real meaning, but it hinders the analysis.

According to some studies, there are weak and strong outliers [15], [16]. Data noise detection offers a wide range of applications. The reduction of noise, for example, results in significantly cleaner data collection that other data mining methods may use. Although noise is not particularly interesting in and of itself, its removal and detection remain a significant concern in the mining industry. As a result, both noise and anomaly detection are critical issues that must be addressed. Throughout the process, methods specific to anomaly detection or noise removal will be identified. The majority of outlier detection techniques, on the other hand, could be utilized for either situation because the distinction is purely conceptual [15].

Anomalies must be correlated to inconsistency, noise and incompleteness. The incompleteness of a database can occur in several ways. For example, values of a given attribute may be missing, an attribute of interest may be missing or an object of interest may be missing. However, the absence of an attribute or object is not always noticed, unless an expert in the problem domain analyzes the database and realizes the lack of data [17].

When various and contradictory copies of the same data emerge in separate places, it is called inconsistent data. In the area of data mining, an inconsistent data is one whose value is outside the domain of the attribute or has a large discrepancy regarding other data. Common examples of inconsistency occur when considering different states of measurement or notation, such as weights given in kilograms (kg) or pounds (€) and distances given in meters or kilometers [17].

Noise has different meanings depending on the context. For example, in videos, a noise is that drizzle in the image, and in radio, it is that interference in the audio signal. Nonetheless, the notion of noise in data mining is closer to the concept of noise in statistics (unexplained variations in a sample) and signal processing (unwanted and usually inexplicable variations in a signal). A noisy data is one that has some variation from its noiseless value, and therefore, noise in the database could lead to inconsistencies. Depending on the noise level, it is not always possible to know whether or not it is present in the data [17].

B. ANOMALY DETECTION

Detecting anomalies (or outliers) is the task of identifying strange data in comparison with others. Anomalies are not necessarily wrong data: they are just spots that stand out among the general population. There is an enormous practical applicability to this problem, from detecting failures to discovering financial fraud, from finding health problems to identifying dissatisfied customers. According Chandola et al. [1], There are three main types of anomalies:

- **Isolated anomalies:** The isolated anomaly (or point anomaly) is an observation point in the dataset that is far away from the rest of the data.
- **Contextual anomalies:** A contextual anomaly is an observation that would be regular in one setting, but abnormal in another.
- **Collective anomalies:** It is necessary to analyze a sequence in order to determine an anomalous behavior.

One can divide the anomaly detection techniques according to their ways of learning, as follows:

- **Supervised anomaly detection:** In this class, both normal and anomalous data are known. The goal is to build a prediction model for both anomaly and normal classes [18].
- **Semi-supervised anomaly detection:** In this type of algorithm, the training only includes ordinary data. Anything not classified that way is tagged as an anomaly [19].
- **Unsupervised anomaly detection:** There is no requirement for training in this scenario. This type of algorithm assumes that normal instances are much more common than anomalies. However, if this assumption fails, the algorithm produces a high rate of false positives [20].

Many of the semi-supervised techniques can be adapted to operate in unsupervised mode using unlabeled data for

training. Such adaptation presumes that there are few but robust anomalies in the test data.

C. NEURAL NETWORKS

A neural network(NN) is a biologically inspired algorithm to learn from data. They are function approximators, particularly useful in Reinforcement Learning when the state space or action space is too large to be known. Their structure has a series of layers, each one composed of one or more neurons. Each neuron produces an output, or activation, based on the outputs of the previous layer and a set of weights [21]. This paper highlights some of them.

1) RECURRENT NEURAL NETWORKS (RNN)

This is a sort of artificial neural network that recognizes patterns in data sequences such as text, genomes, handwriting, spoken word, or data from sensors, stock markets, and government agencies. RNN is a class of neural networks that includes weighted connections within a layer (compared to traditional feed-forward networks, where it connects only to subsequent layers) [22].

2) AUTOENCODER NEURAL NETWORKS (AE)

Autoencoders are neural networks to replicate their input into their output. Then, they compress the data into a latent representation space, from which they rebuild the output. The variational encoding distribution is regularized during the training phase. The goal is to ensure that its latent space has good properties, which allows us to generate new data [23].

3) GENERATIVE ADVERSARIAL NETWORKS (GAN)

These are adversarial deep neural network designs, which are made up of two networks that are pitted against one other. It means the model is up against a formidable foe: a discriminative model that learns to tell whether a sample comes from the model or data distribution. In this type of algorithm, the training only includes ordinary data. Anything not classified that way is tagged as an anomaly [24].

4) DEEP LEARNING

Also known as deep structured learning, is part of a family of learning methods in artificial neural networks with representational learning. Learning can be unsupervised, supervised, or semi-supervised. The deep term alludes to the network's employment of numerous layers. For example, early research demonstrated that while a perceptron cannot be a universal classifier, a network with a non-polynomial activation function and an unbounded width hidden layer may. Deep learning is a recent form that involves an unlimited number of bounded size layers, allowing for practical application and optimization while maintaining theoretical universality under mild conditions. [25]. This paper employs deep learning to designate neural networks with many hidden layers.

D. METRICS

This section summarizes the most used metrics for machine learning model comparison. The selected papers widely employ Accuracy, Sensitivity, Specificity, Precision, F-measure, AUC-ROC, and AUC-PR.

1) ACCURACY

it is the result of correct classifications divided by all classifications, as in (1). It is the most straightforward and widely used metric to measure the performance of a classifier. It is how close a given set of outcomes are to their actual value. However, accuracy is not always a good metric, especially when imbalanced data. The fundamental problem is that when the negative class is dominant, we can achieve high accuracy merely so long as we predict negative most of the time [26].

2) SENSITIVITY

(recall, hit rate, or true positive rate) and **Specificity** (selectivity or true negative rate) mathematically describe the accuracy of a test that reports the presence or absence of a condition. Individuals for which the condition is satisfied are considered positive, and those for which it is not are deemed negative. Sensitivity, as in (2), refers to the probability of a positive test, conditioned on truly being positive. Specificity, as in (3), refers to the likelihood of a negative test, conditioned on truly being negative [27].

3) PRECISION@K

is defined as the proportion of true anomalies in a ranked list of K objects, as in (4). We obtain the ranking list in descending order according to the anomaly scores computed from a specific anomaly detection algorithm. Precision is how close or dispersed the measurements are to each other [28].

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Sensitivity(recall) = \frac{TP}{TP + FN} \tag{2}$$

$$Specificity = \frac{TN}{TN + FP} \tag{3}$$

$$Precision = \frac{TP}{TP + FP} \tag{4}$$

where TP = True positive; FP = False positive; TN = True negative; FN = False negative.

4) F-MEASURE

Precision is also used with recall. The two measures are sometimes used together to provide a single measurement, as in (5). The F-score, F-measure, F1, or F1-Score is precision and recall harmonic mean [27].

$$F1 = 2 \times \frac{Precision \times Sensitivity}{Precision + Sensitivity} \tag{5}$$

5) AUC-ROC

The area under the curve (AUC) is the probability that a randomly chosen anomaly receives a higher score than a randomly chosen ordinary object. It is interpreted as the probability that a randomly chosen anomaly gets a higher score than a randomly chosen ordinary object [28].

6) AUC-PR

It is the area under the curve of precision against recall at different thresholds, and it only evaluates the performance on abnormal samples: the positive class. AUC-PR is computed as the average precision [28].

IV. RELATED WORKS

Conventional detection approaches rely on statistical methods and spatial thresholds and therefore cannot deal with the complex and dynamic nature of anomalies. Recent advances in artificial intelligence using neural network approaches allow the detection of anomalies in more complex typologies because they are able to consider temporal and contextual characteristics of the data.

We found 168 surveys or review papers for anomaly detection in the last five years. Still, only 19 of them are general (not for a specific purpose), only 4 of these papers focus on neural networks, and only one is for machine learning general purposes:

1) Survey on Applying GAN for Anomaly Detection [29].
2) Deep Learning for Anomaly Detection: A Review [30].
3) A Unifying Review of Deep and Shallow Anomaly Detection [31]
4) Machine Learning for Anomaly Detection: A Systematic Review [4]

Other existing research on anomaly detection techniques, such as [32] and [33] only consider neural network-based approaches superficially. Current research developments on neural networks for detecting many anomalies are not incorporated.

This review is different from those described above because it presents an extensive research study on anomaly detection through machine learning techniques focusing on neural networks and covering the period from 2017 to 2021, a period for which, as far as it is known, there is no systematic review yet. Besides [29] focus only on GAN, [30] is not for others neural network, [31] investigates the deepness of networks and [4] is shallow on neural networks.

V. RESULTS AND DISCUSSION

In this section, the reported results are based on the developed protocol. Each subsection explains about the domain with a developed set of machine learning techniques. Table 5 illustrates the overall result of the initial search. They include journal and conference papers.

Many anomaly detection methods have been created for specific applications, while others are more general. So, several papers were mainly focused on detecting anomalies in specific domains of applications or in specific data type, such as Intrusion detection, network anomaly detection, internet of things, image or video processing, crowded scenes, network security or data streams. Theses kind of jobs were rejected. Figure 4 shows accepted papers publication by year.

TABLE 5. Imported studies by source.

Source	Studies
ACM Digital Library	66
IEEE Digital Library	382
Web of Science	361
Scopus	491
Science Direct	122
Total	**1422**
Duplicated	-799
Balance	**623**
Rejected	**547**
Accepted	**76**

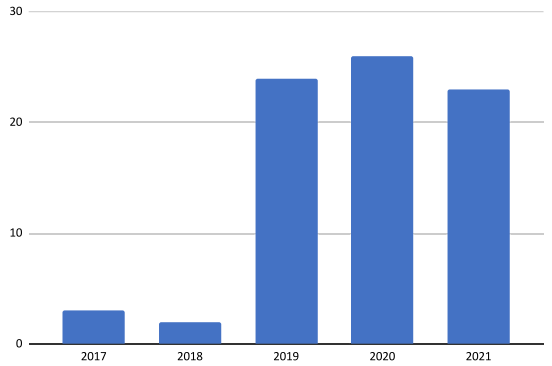


FIGURE 4. Accepted papers (It shows relevant growth in last years).

A. ACCEPTED PAPERS

The following is an extensive overview of all the selected works with highlights of the main characteristics of each.

1) **Towards explaining anomalies: A deep Taylor decomposition of one-class models:** The method proposed an approach for one-class SVMs (OC-SVM), based on the new insight that these models could be rewritten as distance/pooling neural networks. The step of neuralization allows the application of deep Taylor decomposition (DTD) and, besides that, the method is applicable to different common distance-based kernel functions [34].
2) **LRGAN: Visual anomaly detection using GAN with locality-preferred recoding:** To partly avoid latent vectors of normal samples being recoded, the authors presented an improved model using GAN with an adaptive locality-preferred recoding LR (ALR) module, named LRGAN+. The ALR module applies the clustering algorithm to generate a more compact codebook and particularly it helps LRGAN+ to automatically skip the LR module for possible normal samples with a threshold strategy [35].
3) **Multi-Scale One-Class Recurrent Neural Networks for Discrete Event Sequence Anomaly Detection:** the authors proposed OC4Seq, a multi-scale one-class

recurrent neural network for detecting anomalies in discrete event sequences, with the recurrent neural networks (RNNs) embedding the discrete event sequences into latent spaces, where anomalies can be easily detected. Besides, they design a multi-scale RNN framework to capture different levels of sequential patterns at the same time [36].

4) **Error-Bounded Graph Anomaly Loss for GNNs:** To train Graph Neural Networks(GNNs) for anomaly-detectable node representations, the authors proposed an alternative loss function. It uses global grouping patterns discovered from graph mining methods to assess node similarity. It can automatically adjust margins for minority classes based on data distribution [37].
5) **Imbalanced dataset-based echo state networks for anomaly detection:** The traditional echo state network (ESN), a brain-inspired neural computing model, was used in this approach. The error between the input data and the output is smaller when normal data is given to the well-trained network than when abnormal input data is added to the well-trained network. Then, if the difference between the input data and the predicted value exceeds a specific threshold, anomalous behavior is detected [38].
6) **Integration of deep feature extraction and ensemble learning for outlier detection:** In this article, the authors employed stacked autoencoders to extract features and then an ensemble of probabilistic neural networks to do majority voting and find outliers, demonstrating that using autoencoders significantly improved outlier identification performance [39].
7) **Deep anomaly detection with self-supervised learning and adversarial training:** The proposed work was a deep adversarial anomaly detection (DAAD) method, in which an auxiliary task with self-supervised learning is designed first to learn task-specific features, and then a deep adversarial training (DAT) model is built to capture marginal distributions of normal data in various spaces. In addition, to acquire trustworthy detection findings, a majority voting approach is used [40].
8) **Deep Learning for Anomaly Detection:** the authors looked at the state-of-the-art deep learning models, from building block neural network structures like MLP, CNN, and LSTM to more complex structures like autoencoder, generative models (VAE, GAN, Flow-based models), and deep one-class detection models, and show how transfer learning and reinforcement learning can help correct label scatter problems [41].
9) **A machine-learning phase classification scheme for anomaly detection in signals with periodic characteristics:** An novel machine-learning method is proposed here for data with periodic features that explicitly allows for randomly variable period lengths. Training a data-adapted classifier comprised of deep convolutional neural networks for phase classification is used to accomplish a multi-dimensional time series analysis [42].
10) **Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder:** In that paper, the authors offered an unsupervised anomaly detection, which consists of a sliding-window convolutional variational autoencoder (SWCVAE) that can detect anomalies in real-time, both spatially and temporally, by dealing with multivariate time series data [43].
11) **Model fusion of deep neural networks for anomaly detection:** This paper proposed using class weight optimization to train deep neural networks to learn complex patterns from rare anomalies observed in network traffic data. This original model fusion combined two deep neural networks: a binary normal/attack DNN for detecting the availability of any attack and a multi-attack DNN for categorizing the attacks [44].
12) **GP-ELM-RNN: Garson-pruned extreme learning machine based replicator neural network for anomaly detection:** For anomaly detection, the author offered an optimal Replicator Neural Network (RNN) that is optimized using Extreme Learning Machines (ELM) learning and the Garson method. The difficulty of calculating the number of hidden layers is solved by ELM-based RNNs, while the challenge of identifying the optimal number of neurons in the hidden layer is solved by the Garson method [45].
13) **Outlier exposure with confidence control for out-of-distribution detection:** the authors suggested Outlier Exposure with Confidence Control (OECC), a novel method for detecting out-of-distribution (OOD) with OE on image and text classification tasks. the authors further demonstrate that combining OECC with cutting-edge post-training OOD detection approaches like the Mahalanobis Detector (MD) and Gramian Matrices (GM) increases performance [46].
14) **Deep compact polyhedral conic classifier for open and closed set recognition:** In this paper, they proposed a new deep neural network classifier that uses the polyhedral conic classification function to maximize inter-class separation while minimizing intra-class variance. There are two loss terms in the approach, one for each task (maximize and minimize) [47].
15) **Multilayer one-class extreme learning machine:** A multilayer neural network based one-class extreme learning machine (OC-ELM) (in short, as ML-OCELM) was developed in this paper. ML-OCELM uses stacked autoencoders (AE) to leverage an effective feature representation for complex data [48].
16) **Deep convolutional clustering-based time series anomaly detection:** This paper presented an original approach that relies on unlabeled data and uses a 1D-convolutional neural network-based deep autoencoder architecture. the authors divide the autoencoder

latent space into discriminative and reconstructive latent features, then use a Top-K objective to separate the latent space and apply an auxiliary loss based on k-means clustering for the discriminatory latent variables [49].

17) **On the Usage of Generative Models for Network Anomaly Detection in Multivariate Time-Series:** the authors presented Net-GAN, a new method for detecting network anomalies in time series that employs recurrent neural networks (RNNs) and generative adversarial networks (GAN). They also explore the concepts behind generative models to conceive Net-VAE, a complementary approach to Net-GAN, based on variational auto-encoders (VAE) [50].
18) **MAMA Net: Multi-Scale Attention Memory Autoencoder Network for Anomaly Detection:** The authors proposeed a Multi-scale Attention Memory with hash addressing Autoencoder network (MAMA Net). the authors designed a hash addressing memory module that explores abnormalities to produce greater reconstruction error for classification, and they connected the mean square error (MSE) with Wasserstein loss to improve the encoding data distribution, and created the multi-scale global spatial attention block, which could be attached to any network as sampling, upsampling, and downsampling functions [51].
19) **A novel multivariate time-series anomaly detection approach using an unsupervised deep neural network:** In this paper, the authors proposed a multilayer convolutional recurrent autoencoded anomaly detector (MCRAAD), which was an unsupervised deep learning method. They used the data in the sliding window to calculate the feature matrix sequence, a multilayer convolutional encoder to extract the feature matrix sequence's characteristics, several ConvLSTM units to obtain the feature matrix's time relations, and a convolutional decoder to reconstruct the feature matrix sequence [52].
20) **Hybrid discriminator with correlative autoencoder for anomaly detection:** For anomaly detection, the authors suggested a hybrid discriminator with a correlative autoencoder. The discriminator estimates the conditional probability density function in the suggested framework, while the autoencoder enhances the capacity to manage the reconstruction error. [53]
21) **Unsupervised Boosting-Based Autoencoder Ensembles for Outlier Detection:**The authors created the Boosting-based Autoencoder Ensemble approach (BAE). It was an unsupervised ensemble method. This method constructs an adaptive cascade of autoencoders to get better outcomes, very close to boosting. It trains the autoencoder components in sequence by performing a weighted sampling of the data, intended to reduce the number of anomalies during training and to insert diversity in the ensemble. [54]
22) **HIFI: Anomaly Detection for Multivariate Time Series with High-order Feature Interactions:** The authors offered a novel anomaly detection approach for multivariate time series with HIgh-order Feature Interactions (HIFI). It created multivariate feature interaction graph and used the graph convolutional neural network to achieve high-order feature interactions, modeling the long-term temporal dependencies by attention mechanisms and using a variational encoding technique to improve the model [55].
23) **Activation Anomaly Analysis:** The suggested method demonstrated that hidden activation values contain information that can be used to differentiate between normal and abnormal samples. In a purely data-driven end-to-end model, three neural networks were combined in the approach. The alarm network determined if a particular sample is normal based on the activation values in the target network. [56]
24) **TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks:** This article presented TadGAN, an unsupervised anomaly detection method based on Generative Adversarial Networks. The authors employed LSTM Recurrent Neural Networks as basic models for Generators and Critics to capture the temporal correlations of time series distributions. To enable effective time-series data reconstruction, TadGAN was trained with cycle consistency loss [57].
25) **TAnoGAN: Time Series Anomaly Detection with Generative Adversarial Networks:** In this work, the authors suggested the method TAnoGan, an unsupervised method based on Generative Adversarial Networks (GAN) for detecting anomalies in time series when just a few data points are available [58].
26) **A Transfer Learning Framework for Anomaly Detection Using Model of Normality:** Deep features could be extracted using a Convolutional Neural Network (CNN), and anomalies could be detected using a comparable measure between extracted features and a defined model of normality. Here, the authors presented a method for determining the decision threshold that improves detection accuracy and a transfer learning framework for anomaly detection based on a Model of Normality (MoN) similarity measure [59].
27) **Novelty Detection Through Model-Based Characterization of Neural Networks:** The authors proposed a model-based characterization of neural networks to detect new input types and conditions. According to them, most existing research has focused on activation-based representations to detect abnormal inputs, and back-propagated gradients have been used to formulate the significance of the perspective in novelty detection [60].
28) **USAD: UnSupervised Anomaly Detection on Multivariate Time Series:** The authors proposed a rapid and stable technique based on adversely trained

autoencoders and named UnSupervised Anomaly Detection for Multivariate Time Series (USAD). The architecture of the autoencoder made it able to learn unsupervised and using adversarial training and its architecture allows it to isolate anomalies while giving fast training [61].

29) **Unsupervised anomaly detection with LSTM neural networks:** Given variable-length data sequences, the authors first passed them through a long short-term memory (LSTM) neural network-based structure and obtained fixed-length sequences. Then they found a decision function based on the one-class support vector machines (OC-SVMs) and support vector data description (SVDD) algorithms. Finally, they trained and optimized all the parameters using highly effective gradient and quadratic programming-based training methods. It was also possible to apply this approach to the gated recurrent unit (GRU) architecture by replacing the LSTM-based structure with the GRU-based structure [62].
30) **Deep Active Learning for Anomaly Detection:** In this work, the authors presented a new layer that could be attached to any deep learning unsupervised anomaly detection model to turn it into an active method. They showed results using Multi-layer Perceptrons and Autoencoder architectures improved with the proposed active layer [63].
31) **DeepAlign: Alignment-Based Process Anomaly Correction Using Recurrent Neural Networks:** DeepAlign was a new approach based on recurrent neural networks and bidirectional beam search. It had two recurrent neural networks, one that reads sequences of process executions from left to right, while the other reads the sequences from right to left. By combining them, the authors showed that it is possible to calculate sequence alignments to detect and correct anomalies [64].
32) **Arcade: A rapid continual anomaly detector:** This study addressed a situation in which the only examples given for training was from the regular class. The authors characterized it as a meta-learning issue and defined it as a continuous anomaly detection (CAD) learning problem. As a result, they offered A Rapid Continual Anomaly Detector (ARCADe), a method for training neural networks to be robust to the main challenges of this novel learning problem, such as catastrophic forgetting and overfitting to the majority class [65].
33) **Latent feature decentralization loss for one-class anomaly detection:** The suggested method aims to disseminate the encoder's latent feature over multiple spaces, allowing it to generate images comparable to the standard class for any input. So, a decentralization term based on the dispersion measure for latent vectors is also added to the existing mean-squared error loss. The authors limited the latent space by creating a dispersion measure upper bound based on a decentralization loss term. When the given test image is unknown, the reconstruction error increases [66].
34) **Deep multi-sphere support vector data description:** In this paper, the authors offered Deep Multi-sphere Support Vector Data Description, which optimized both the deep network and anomaly detection algorithms' goals by combining standard data with a multimodal distribution into multiple data enclosing hyperspheres with minimum volume provides valuable and discriminative features [67].
35) **The Elliptical Basis Function Data Descriptor (EBFDD) Network: A One-Class Classification Approach to Anomaly Detection:** The paper introduced the Elliptical Basis Function Data Descriptor (EBFDD) network, based on Radial Basis Function (RBF) neural networks, as a one-class classification method for anomaly detection. The EBFDD network makes use of elliptical basis functions to learn complex decision boundaries while maintaining the benefits of a shallow network [68].
36) **Anomaly Detection by Learning Dynamics from a Graph:** The authors offered a method for learning Spatio-temporal properties called dynamics to forecast the evolution of graphs. It included two steps: extracting spatial features from static graphs from various times and learning temporal features from the time-varying structure. They identified the dynamic anomaly by predicting the affinity score for a node in a dynamics graph rather than predicting overall changes [69].
37) **A deep reinforcement learning based homeostatic system for unmanned position control:** This research proposed a novel bio-inspired homeostatic technique based on a Receptor Density Algorithm (an artificial immune system-based anomaly detection application) and a Plastic Spiking Neuronal model to capture the randomness of the environment. Deep Reinforcement Learning (DRL) was used in conjunction with the hybrid model described above. [70]
38) **Deep Autoencoders with Value-at-Risk Thresholding for Unsupervised Anomaly Detection:** The authors presented an incremental learning strategy in which the regular data deep autoencoding (DAE) model is learned and utilized to identify anomalies. They applied a unique thresholding approach based on the value at risk (VaR) for detecting them, then compared the resulting convolutional neural network (CNN) against various subspace methods [71].
39) **Computation of person re-identification using self-learning anomaly detection framework in deep-learning:** This paper proposed a self-Learning anomaly detection application. To begin, it got metadata from the unsupervised data clustering module (DCM), which analyzes the pattern of monitoring data and could find unforeseen anomalies by enabling self-learning. The DCM's pattern is then transferred to a

supervised data regression and classification module (DRCM) [72].

40) **Learning Deep Features for One-Class Classification:** The authors described a new deep-learning-based approach for one-class transfer learning in one-class categorization. It provided descriptive features while preserving a low intra-class variance in the feature space for the given class by operating on top of a convolutional neural network (CNN) of choice. Two loss functions (compactness and descriptiveness) and a parallel CNN architecture were proposed to achieve this goal [73].
41) **Performance Analysis of Out-of-Distribution Detection on Various Trained Neural Networks:** When Deep Neural Networks (DNN) were exposed to previously unseen out-of-distribution samples, the authors faced a typical difficulty. Here, they focused on two supervisors on two well-known DNNs with different training configurations and found that the quality of the training technique increases the outlier identification performance [74].
42) **Sequential anomaly detection using inverse reinforcement learning:** The authors proposed an inverse reinforcement learning (IRL) framework for sequential anomaly detection and a Bayesian technique for IRL. The approach took the series of actions of a target agent as input, and the reward function inferred by IRL then understood the agent's normal behavior. It represented a reward function using a neural network and analyzed whether a new observation from the target agent follows a regular pattern [75].
43) **Cyclostationary statistical models and algorithms for anomaly detection using multi-modal data:**Using a Deep Neural Network-based object detector to extract counts of objects and sub-events from the data was offered as a framework for detecting anomalies in multimodal data. In order to model regular patterns of behavior in count sequences, a cyclo-stationary model was developed. The anomaly detection challenge is defined as finding deviations from learned cyclo-stationary behavior [76].
44) **Concept learning through deep reinforcement learning with memory-augmented neural networks:** The authors presented a memory-augmented neural network inspired by the human concept learning process. The training teaches how to discriminate between samples from various classes and group examples of the same type together. In addition, they suggested a sequential procedure in which the network should determine how to recall each sample at each stage [77].
45) **A study of feature reduction techniques and classification for network anomaly detection:** Principal Component Analysis (PCA), Artificial Neural Network (ANN), and Nonlinear Principal Component Analysis (NLPCA) are the three reduction methodologies explored and analyzed in this paper. For the actual and reduced datasets, the classifiers Decision Tree (DT), Support Vector Machine (SVM), K Nearest Neighbor (KNN), and Naive Bayes (NB) were also investigated. In addition, new performance measurement metrics, such as the Classification Difference Measure (CDM), Specificity Difference Measure (SPDM), Sensitivity Difference Measure (SNDM), and F1 Difference Measure (F1DM), have been defined and were being used to compare the outcomes on actual and reduced datasets [78].
46) **MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks:** In this work, the authors proposed an unsupervised multivariate method based on Generative Adversarial Networks (GANs), using the Long-Short-Term-Memory Recurrent Neural Networks (LSTM-RNN) as the base models in the GAN framework to capture the temporal correlation of time series distributions. The Multivariate Anomaly Detection with GAN (MAD-GAN) framework considers the entire set of variables simultaneously to capture latent interactions between variables. They also use a new anomaly score called DR-score to detect anomalies through discrimination and reconstruction [79].
47) **Outlier detection for time series with recurrent autoencoder ensembles:** The authors proposed two methods for detecting outliers in time series using recurrent autoencoder ensembles. The autoencoders are made up of sparsely-connected recurrent neural networks (S-RNNs). These methods permitted several autoencoders to be created with varied neural network connection architectures. This ensemble-based technique improved overall detection quality by limiting the consequences of overfitting some autoencoders to outliers [80].
48) **An Approximate Bayesian Long Short-Term Memory Algorithm for Outlier Detection:** In this study, the authors presented an Ensemble Kalman Filter-based approximate estimation of weights uncertainty, which was easily scalable to a high number of weights. Besides, they optimized the covariance of the noise distribution in the ensemble update step using maximum likelihood estimation [81].
49) **DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series:** The authors described a new deep learning-based time series data technique (DeepAnT). It learned the data distribution used to forecast the expected behavior of a time series using unlabeled data. DeepAnT consists of two modules. First, the predictor module projects the next time stamp on the defined horizon using a deep convolutional neural network (CNN). The predicted value is then provided to the anomaly detector module, which assigns a normal or abnormal label to the time stamp [82].

50) **Outlier detection with autoencoder ensembles:** For unsupervised anomaly detection, in this paper the authors introduced autoencoder ensembles. The main idea was to change the autoencoder's connectivity design at random to improve performance substantially. They also integrated this methodology with an adaptive sampling strategy to improve the efficiency of the approach [83].
51) **Training autoencoder using three different reversed color models for anomaly detection:** This paper introduced Autoencoders (AE) as an anomaly detector. The suggested AE was built on a convolutional neural network with three different color models: Hue Saturation Value (HSV), Red Green Blue (RGB), and their own model (TUV), and it is trained using both normal and anomalous data. The trained AE reconstructs normal images unchanged, while anomalous images are rebuilt in the opposite direction [84].
52) **Detection of Thin Boundaries between Different Types of Anomalies in Outlier Detection Using Enhanced Neural Networks:** the authors defined new types of anomalies for improving a better detection of the boundary between different types of anomalies and basic methods were introduced to detect these defined anomalies in supervised and unsupervised datasets. The Multi-Layer Perceptron Neural Network (MLP) was upgraded using the Genetic Algorithm to identify the new defined anomalies with more precision, resulting in a lower test error than the calculated for the conventional MLP [85].
53) **NADS-RA: Network Anomaly Detection Scheme Based on Feature Representation and Data Augmentation:** This paper offered a Network Anomaly Detection Scheme based on feature representation and data augmentation (NADS-RA). To begin, the Re-circulation Pixel Permutation approach was intended to be used as a feature representation strategy for creating images. Then, an image-based augmentation strategy was designed to produce augmented images according to the distribution characteristics of rare anomaly images with the help of Least Squares Generative Adversarial Network, which softens the effect of imbalanced training data. Lastly, NADS-RA was implemented on the Convolutional Neural Network classification model [86].
54) **An improved BiGAN based approach for anomaly detection:** In this study, the authors implemented Bidirectional GAN (BiGAN) architecture, considering it as a one-class anomaly detection algorithm. They presented two different training methodologies for BiGAN by adding extra training stages, because the generator and discriminator are heavily dependent on each other during the training phase [87].
55) **Anomalous Example Detection in Deep Learning: A Survey:** This review provided a well-organized and thorough overview of anomaly detection research for Deep Learning (DL) based applications. The authors provided a classification for existing techniques based on their underlying assumptions and adopted approaches. They discussed different techniques in each of the categories and provide their relative strengths and weaknesses [88].
56) **Deep Autoencoders and Feedforward Networks Based on a New Regularization for Anomaly Detection:** Here, the authors overviewed two architectures that push the limits of model accuracy for anomaly detection and intrusion classification, the Feedforward Neural Network (FNN) and Variational Autoencoder (VAE). They provided an overview of the architecture model, including training approaches, hyperparameters, regularization, and other aspects. Furthermore, they created a new regularization technique based on the standard deviation of weight values, which they applied to both models [89].
57) **Convolutional Neural Network-Based Discriminator for Outlier Detection:** The authors suggested a method for producing training datasets that useed a small set of reliable data to train the discriminator. the authors evaluated the discriminator's performance using multiple benchmark datasets and noise ratios, and the authors used a Convolutional Neural Network (CNN) for the noise discriminator. They introduced random noise into each dataset and train discriminators to clean it up [90].
58) **Online anomaly detection with sparse Gaussian processes:** The method of sparse Gaussian processes with Q-function (SGP-Q) is proposed in this study. The SGP-Q employs sparse Gaussian processes (SGPs), which have a lower time complexity than Gaussian processes (GPs), allowing for substantially faster online anomaly detection. If the Q-function was used correctly, the SGP-Q may adapt well to concept drift, where data properties and anomalous behaviors change with time [91].
59) **Anomaly detection with inexact labels:** The authors proposed a supervised method for data with inexact anomaly labels, where each label indicates that at least one instance in the set is anomalous. They defined the inexact AUC, which is an extension of the Area Under the ROC Curve (AUC), to quantify performance. The strategy improved the smooth approximation of the inexact AUC while decreasing scores for non-anomalous occurrences by training an anomaly score function. They used an unsupervised anomaly detection method based on neural networks, such as Autoencoders, to model the score function [92].
60) **Skip-GANomaly: Skip Connected and Adversarially Trained Encoder-Decoder Anomaly Detection:** The authors introduced an unsupervised model, trained only on the non-anomalous samples. The method employed an encoder-decoder Convolutional Neural Network with skip connections to completely capture

the multi-scale distribution of the expected data in image space. Besides, an adversarial training scheme provides superior reconstruction within image space and a lower-dimensional vector space encoding. Furthermore, minimizing the reconstruction error metric during the training helped the model learn the distribution of normality, and higher reconstruction metrics indicate an anomaly [93].

61) **Deep One-Class Classification Using Intra-Class Splitting:** This paper introduced a generic method that enables to use of conventional deep neural networks for one-class classification, where only samples of one regular class are available for training. During inference, a closed and rigid decision border around the training samples is desired, which is unattainable with traditional binary or multi-class neural networks. This method can use a binary loss and creates a subnetwork for distance constraints in the latent space by separating data into typical and atypical normal subsets [94].
62) **Anomaly detection based on mining six local data features and BP neural network:** The authors presented a model that used six local data features as the input to a back-propagation (BP) neural network. The six mined local data features give subtle insight into local dynamics by describing the local monotonicity, convexity/concavity, inflection property, and peak distribution of one KPI time series through vectorization description on a normalized dataset. This was in contrast to some traditional statistics data characteristics describing the entire variation situation of one sequence [95].
63) **An Empirical Evaluation of Deep Learning for Network Anomaly Detection:** Their preliminary studies revealed a significant degree of non-linearity in network connection data. Furthermore, their approach explained why traditional algorithms like Adaboosting, SVM, and Random Forest struggled to enhance anomaly detection performance. In this research, the authors created and tested deep learning models based on Fully Connected Networks (FCNs), Variational AutoEncoders (VAE), and Sequence-to-Sequence (Seq2Seq) structures [96].
64) **Optimized fuzzy min-max neural network: An efficient approach for supervised outlier detection:** The authors modified the Fuzzy min-max Neural Network (FMNbasic)'s architecture to represent learned knowledge in a compact, coarse-grained manner similar to human thinking. The proposed method was known as the fuzzy min-max neural network with knowledge compaction (FMN-KC), and its potential for supervised outlier detection was shown using available online datasets [97].
65) **Limiting the reconstruction capability of generative neural network using negative learning:** Generative models with only a single input type are beneficial for applications like constraint handling, noise reduction, and anomaly detection. This paper presented a method for employing negative learning to limit the network's generative capabilities. For the desired input, the approach searched the solution in the gradient direction and for the undesired input, such as anomalies, in the opposite direction. [98].
66) **Robust, Deep and Inductive Anomaly Detection:** This article addressed in a single model both difficulties in overcoming PCA's limitations of being sensitive to input perturbations and searching for a linear subspace that reflects normal behavior. This method, the robust Autoencoder, learned a nonlinear subspace that captures most data points while allowing for random corruption of specific data. Moreover, it was easy to learn and takes advantage of recent Deep Neural Network optimization breakthroughs [99].
67) **An Anomaly Event Detection Method Based on GNN Algorithm for Multi-data Sources:** To address the known problems of inadaptability of multi-source data in anomaly detection, the authors designed a new method based on it in this paper. First, they used a spectral clustering approach to extract features from numerous data sources and combine them. They then executed an improved anomaly social event detection, showing the threatening events, utilizing the power of a Deep Graph Neural Network (Deep-GNN) [100].
68) **Few-shot network anomaly detection via cross-network meta-learning:** The authors addressed the few-shot network anomaly detection problem by developing Graph Deviation Networks (GDN). It was a novel family of neural graph networks that could enforce statistically significant differences between abnormal and normal nodes on a network using a limited number of labeled abnormalities. They also included a new cross-network meta-learning technique in the proposed GDN to enable few-shot network anomaly detection by transferring meta-knowledge from auxiliary networks [28].
69) **Anomaly Detection of Time Series with Smoothness-Inducing Sequential Variational Auto-Encoder:** The authors introduced a smoothness-inducing Sequential Variational Auto-encoder (VAE) (SISVAE) approach for multidimensional time series robust estimation and anomaly detection. The model was based on VAE, and for both the generating and inference models, it was fulfilled by a Recurrent Neural Network to capture latent temporal features of time series. They offered a smoothness-inducing prior over potential estimations as a regularizer that penalized nonsmooth reconstructions for achieving robust density estimation. They used a novel stochastic gradient variational Bayes estimator to learn their model efficiently, and they investigated two decision criteria for anomaly detection: reconstruction probability and reconstruction error [101].

70) **Deep End-to-End One-Class Classifier:** The authors presented an adversarial training strategy for detecting out-of-distribution samples in an end-to-end trainable deep model. They achieved this by combining the training of two Deep Neural Networks (R and D). D serves as the discriminator, while R assists D in defining a probability distribution for the target class by providing adversarial instances during training and collaborates with it during testing to discover anomalies [102].
71) **A survey of deep learning-based network anomaly detection:** In this paper, the authors gave an overview of Deep Learning methodologies, such as restricted Boltzmann machine-based deep belief networks, Deep Neural Networks, and Recurrent Neural Networks, as well as machine learning techniques applicable to network anomaly detection [103].
72) **Unsupervised Anomaly Detection in Stream Data with Online Evolving Spiking Neural Networks:** Their goal was to modify the Online evolving Spiking Neural Network (OeSNN) classifier such that it could successfully detect anomalies without having access to labeled training data. As a result, the authors developed a method called Online evolving Spiking Neural Network for Unsupervised Anomaly Detection (OeSNN-UAD), which, unlike OeSNN, worked unsupervised and does not divide output neurons into discrete decision classes. Instead, it used three new modules: Generation of output values of candidate output neurons, Anomaly classification, and Value correction [104].
73) **Decoupling Representation Learning and Classification for GNN-based Anomaly Detection:** The authors investigated additional options for decoupling node representation learning and classification for anomaly detection than joint training, based on graph neural network (GNN) and self-supervised learning (SSL) on graphs. They showed that decoupled training using existing graph SSL schemes might deteriorate when the behavior patterns and the label semantics become highly inconsistent. They propose an effective graph SSL scheme, called Deep Cluster Infomax (DCI), that clusters the entire graph into multiple parts to capture the fundamental graph attributes in more concentrated feature spaces [105].
74) **A Unifying Review of Deep and Shallow Anomaly Detection:** The authors aimed to identify the common principles and assumptions often made implicitly by various deep learning methods, such as generative models, one-class classification, and reconstruction. They drew linkages between classic and modern deep approaches and explained how this relationship might cross-fertilize or extend in both directions. They also provided an empirical assessment of the most often used approaches [31].
75) **EBOD: An ensemble-based outlier detection algorithm for noisy datasets:** The authors offered an unsupervised ensemble-based outlier detection (EBOD) strategy considering the ensemble of different algorithms. Each selected detector is exclusively responsible for finding a limited number of the most apparent outliers from their specific point of view. Compared to employing a single detector, having an ensemble of weak detectors reduces the possibility of bias. Forward-backward search was used to find the best detector combination [106].
76) **Deep Structured Cross-Modal Anomaly Detection:** The authors proposed a deep neural network-based cross-modal anomaly detection approach (CMAD) in this paper. First, they trained a deep structured model to represent features from different modalities and then project them into a latent feature space. After that, they ''pulled'' the projections of a pair of instances from different modalities together if their cross-modal patterns were consistent. Otherwise, they ''push'' them apart. Then they measure the distances between different modalities to identify cross-modality anomalies [107].

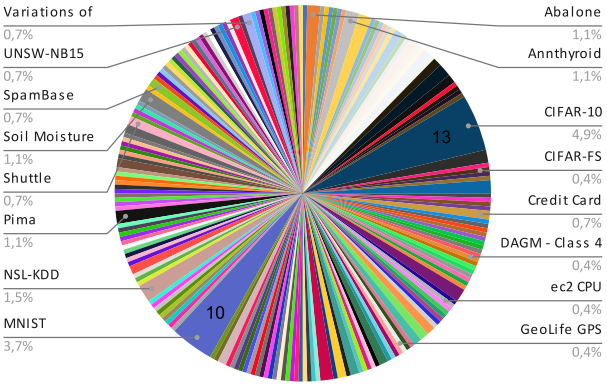


FIGURE 5. Most used datasets.

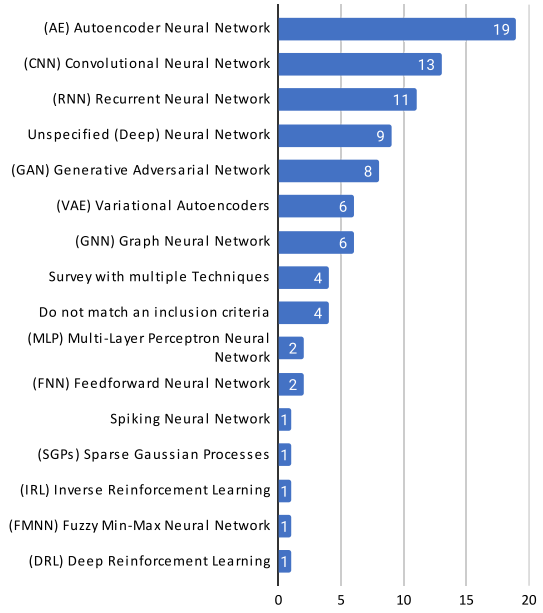


FIGURE 6. Detailed techniques frequency.

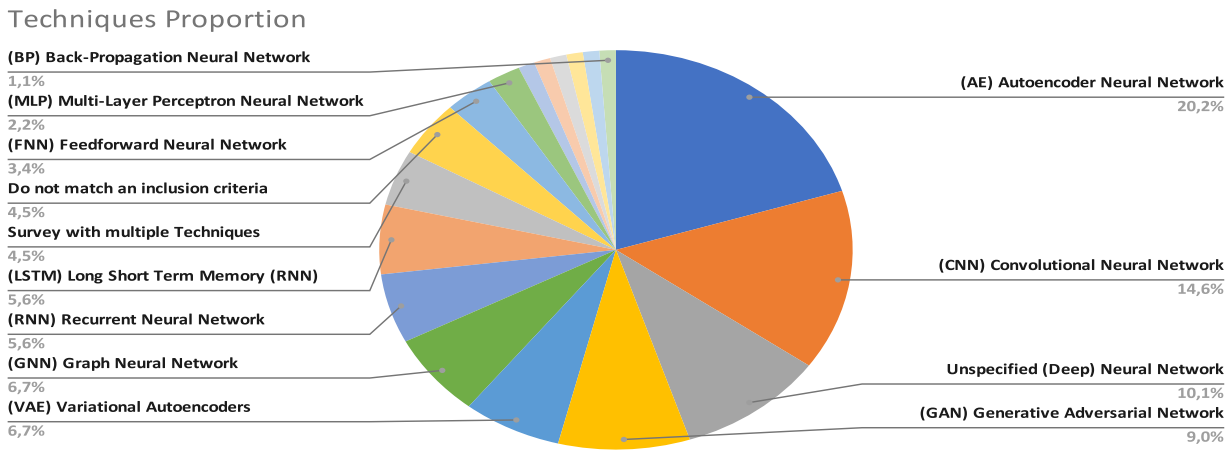


FIGURE 7. Neural network frequencies.

B. DATASET, NETWORK AND PERFORMANCE

Figure 5 shows the Canadian Institute for Advanced Research (CIFAR) [108] and Modified National Institute of Standards and Technology database (MNIST) [109] as the most used datasets. CIFAR (or CIFAR-10) is a collection of 60000 32 × 32 color images in 10 different image classes, and MNIST is an extensive database of handwritten 28 × 28 pixel bounding box digits. Both are commonly used to train machine learning algorithms. Table 6 presents all selected papers with employed neural network techniques, datasets, and their respective performance metric.

C. WHAT KINDS OF NEURAL NETWORKS ARE USED TO OUTLIER DETECTION?

This research question aims to specify the neural networks used to detect anomalies within the period covered by survey will be addressed. As a fundamental point, the networks most used in detecting anomalies are identified along with a brief assessment.

The most Common neural networks found:

- AE: Autoencoder Neural Network
- CNN: Convolutional Neural Network
- RNN: Recurrent Neural Network(LSTM)
- GAN: Generative Adversarial Network

AE: Autoencoders can figure out correlated input features. This algorithm will find some of those (linear or not) correlations. Indeed, an autoencoder learns a low-dimensional representation very close to PCAs. Since the algorithm learns the correlations, as shown in figure 6, it is widely used to discover anomalies.

RNN: Recurrent Neural Network includes some othres subtypes like LSTM, Long Short-Term Memory, GRU, Gated Recurrent Unit Neural Network, and HTM, Hierachical Temporal Memory. LSTM represents more than 60% of all RNN. Anomaly detection algorithms using neural networks could be separated into three main categories: Feature Extraction, Normality Learning, Abnormality threshold [30].

Feature extraction algorithms, as CNN, simplify the data, usually by reducing the number of dimensions. The lower-dimensional space usually highlights hidden anomalies that reduce the false-positive rate. Neural networks, notably deep learning ones, demonstrate substantially better ability to extract complex features and nonlinear relationships. The features extracted by these models preserve the central information that separates anomalies from normal cases. This kind of network performs better than linear methods and is easy to build and run. On the other hand, when the correlation between characteristics is very weak, it is common for this network to be taken to local minimums. In normality learning, networks are forced to capture the underlying regularities of the data. These algorithms assume that normal instances are easier to downsize or structure than anomalies. The Abnormality threshold is not dependent on the existing outliers score. Instead, the neural network directly learns the anomalies. [110].

D. WHAT ARE NEURAL NETWORKS STRENGTHS FOR OUTLIER DETECTION

This section will address this research question that aims to identify the main characteristics of neural networks used to detect anomalies, highlighting their strengths and limitations.

One of the most explored hypotheses is that feature representations extracted by deep networks preserve discriminatory information that helps separate anomalies from normal instances. One of the approaches in this direction is to use pre-trained deep learning models, such as AlexNet, VGG, and ResNet [111], [112], [113], to extract low-dimensional characteristics. This line is widely used in research to detect anomalies in complex high-dimensional data, such as images and videos.

Compared to popular dimension reduction methods in anomaly detection, such as principal component analysis and random projection, deep networks have demonstrated a substantially better ability to extract features in linear and nonlinear relationships [110].

Consider combining different outlier detection techniques, in which each of the selected detectors is only responsible

TABLE 6. Datasets and Metrics compiled from the researched articles.

Paper	Network type	Dataset	Metric	Value
Montavon *et al 2020* [34]	(AE) Autoencoder Neural Network	MNIST CIFAR-10 Personal atacks dataset (Detox)	Not available	Not available
Li *et al 2021* [35]	(GAN) Generative Adversarial Network	MNIST CIFAR-10 Real-world industrial Fasteners	ROC-AUC	0.9828 0.7802 0.9583
Tang *et al 2021* [36]	(RNN) Recurrent Neural Network	HDFS RUBiS BGL	F1-Score	0.955 0.987 0.704
Jiang *et al 2020* [37]	(GNN) Graph Neural Network	Bitcoin-Alpha Tencent-Weibo	F1-Score	0.7568 0.9042
Song *et al 2020* [38]	(RNN) Recurrent Neural Network	Real-world clinical Heart Rate	Not available	Not available
Ghosh *et al 2019* [39]	(AE) Autoencoder Neural Network	PenDigits OptDigits Forest Cover MNIST HTRU2 SatImage-2 Credit Card Speech	ROC-AUC F1-Score G-Mean	0.9923 0.9684 0.9324 0.9454 0.9262 0.9589 0.9421 0.8769 0.9656 0.8951 0.9335 0.9453 0.9209 0.9432 0.7760 0.8007 0.9659 0.8976 0.9335 0.9454 0.9210 0.9433 0.7884 0.8038
Hengel *et al 2019* [117]	(GAN) Generative Adversarial Network	MNIST KDDCUP Annthyroid Arrhythmia SpamBase WDBC	F1-Score ROC-AUC Average Precision (AP) Average Accuracy (ACC)	0.9851 0.8700 0.5422 0.6111 0.6676 0.8889 0.9971 0.9715 0.7019 0.8009 0.7307 0.9000 0.9723 0.7540 0.4708 0.5281 0.5480 0.8247 0.9971 0.9772 0.9467 0.9060 0.7301 0.9753
Chawla *et al 2019* [33]	Survey with multiple Techniques	Do not apply	Do not apply	Do not apply
Schotten *et al 2019* [42]	(CNN) Convolutional Neural Network	Cardiology (ECG) Industrial network dataset for cyber attack research (SCADA) Synthetic waveform	Average Accuracy (ACC)	0.79 Not available 0.99
Lai *et al 2020* [43]	(VAE) Variational Autoencoders	KUKA KR6R 900 SIXX Robot	Precision Recall F1-Score PR-AUC	0.9654 0.8206 0.8871 0.9093

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

Wazir *et al 2021* [44]	Real-world network traffic (ZYELL)	Recall Precision F1-Score β-Score False Alarm Rate (FAR)	0.9033 0.4800 0.5533 0.6518 0.0230		
Ahmad *et al 2019* [45]	(RNN) Replicator Neural Network	Lymphography Post-Operative Wisconsin Breast Cancer Page-blocks Credit Card Fraud Forest Cover KDD-Cup99	Accuracy (Jaccard Similarity) Accuracy	0.9864 0.9792 0.9999 0.9999 0.8333 0.8717 0.9857 0.5427	0.9111 0.9934 0.9982 0.8461 0.8857 0.9100
Wang *et al 2021* [46]	Unspecified (Deep) Neural Network	SVHN CIFAR-10 CIFAR-100	FPR95 ROC-AUC PR-AUC	0.0003 0.2889 0.9999 0.9180 0.9955 0.7150	0.0656 0.9840 0.9308
Ozturk *et al 2021* [47]	(CNN) Convolutional Neural Network	PASCAL VOC CIFAR-100 FaceScrub CIFAR-10 SVHN	Average Precision (AP) Average Accuracy (ACC) ROC-AUC	0.8250 0.8317 0.9819 0.8770 0.9320	
Yang *et al 2019* [48]	(AE) Autoencoder Neural Network	Spectfheart Arrhythmia Sonar Liver Ecoli Diabetes Breast Abalone Letter Pendigits Optical digits Magic Satimage	F1-Score	0.5870 0.7750 0.7080 0.9440 0.8926 0.9535 0.9412	0.7870 0.5850 0.6810 0.7140 0.9324 0.8622
Ding *et al 2021* [49]	(CNN) Convolutional Neural Network	Tennessee Eastman	F1-Score	0.5004	
Gómez *et al 2021* [50]	(GAN) Generative Adversarial Network	CPS SYN-NET	True Positive Rate (TPR) False Positive Rate (TPR)	0.70 0.90 < 0.01 < 0.01	
Wu *et al 2021* [51]	(AE) Autoencoder Neural Network	COVID-19 CT Images COVID-19 X-Ray Images RIDER Neuro MRI	Recall Accuracy F1-Score ROC-AUC	0.901 $\pm$ 0.06 0.920 $\pm$ 0.02 0.873 $\pm$ 0.03 0.909 $\pm$ 0.05 0.938 $\pm$ 0.04 0.847 $\pm$ 0.05 0.905 0.929 0.859 0.957 0.969 0.883	

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

Wang *et al 2021* [52]	(CNN) Convolutional Neural Network (LSTM) Long Short-Term Memory (AE) Autoencoder Neural Network	Synthetic Time-series Real-world House Monitoring	Precision Recall F1-Score G-Mean	0.986 0.880 0.806 0.825 0.887 0.852 0.897 0.908
Kyung *et al 2021* [53]	(AE) Autoencoder Neural Network	MNIST Fashion MNIST COIL-100 CIFAR-10	ROC-AUC	0.977 0.887 0.999 0.692
Stilo *et al 2021* [54]	(AE) Autoencoder Neural Network	UCI Machine Learning Repository	PR-AUC	46.2
Zheng *et al 2021* [55]	(GNN) Graph Neural Network	Server Machine Dataset (SMD) Soil Moisture Active Passive (SMAP) Mars Science Laboratory Rover (MSL)	F1-Score	0.9546 0.9708 0.9773
Valera *et al 2021* [56]	(AE) Autoencoder Neural Network	Variations of MNIST EMNIST NSL-KDD Credit Card Transactions CSE-CIC-IDS2018	Average Precision (AP) ROC-AUC	0.98 0.99 0.96 0.78 0.89 0.99 0.99 0.96 0.96 0.94
Veeramachaneni *et al 2020* [57]	(GAN) Generative Adversarial Network	Mars Science Laboratory (MSL) Soil Moisture Active Passive (SMAP) Yahoo S5 - A1 Yahoo S5 - A2 Yahoo S5 - A3 Yahoo S5 - A4 NAB-Art NAB-AdEx NAB-AWS NAB-Traf NAB-Tweets	F1-Score	0.623 0.704 0.800 0.867 0.685 0.600 0.800 0.800 0.644 0.486 0.609
Nayak *et al 2020* [58]	(GAN) Generative Adversarial Network	46 datasets of NAB	Accuracy Precision Recall F1-Score Cohen Kappa ROC-AUC	Not available
Shami *et al 2020* [59]	(CNN) Convolutional Neural Network	DAGM - Class 1 DAGM - Class 2 DAGM - Class 3 DAGM - Class 4 DAGM - Class 5 DAGM - Class 6 DAGM - Class 7 DAGM - Class 8 DAGM - Class 9 DAGM - Class 10	ROC-AUC	0.80 1.00 0.92 0.99 1.00 0.97 0.87 0.94 0.98 0.85
AlRegib *et al 2020* [60]	(VAE) Variational Autoencoders	MNIST Fashion-MNIST CIFAR-10 CURE-TSR	ROC-AUC	0.953 0.918 0.582 0.746
Zuluaga *et al 2020* [61]	(AE) Autoencoder Neural Network	Secure Water Treatment (SWaT) Water Distribution (WADI)	Precision	0.9870 0.6451 0.9314 0.7697 0.8810 0.7448

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

		Server Machine Dataset (SMD) Soil Moisture Active Passive (SMAP) Mars Science Laboratory Rover (MSL) Internal dataset (Orange)	Recall F1-Score	0.7402 0.3220 0.9617 0.9831 0.9786 0.6428 0.8460 0.4296 0.9382 0.8186 0.9109 0.6901
Kozat and Ergen *2020* [62]	(LSTM) Long Short-Term Memory (RNN)	Occupancy Hong Kong Exchange (HKE) HTTP Alcoa Stock Price	ROC-AUC (Average)	0.8383 0.9037 0.9989 0.9054
Ziviani *et al 2020* [63]	(AE) Autoencoder Neural Network + (MLP) Multi-Layer Perceptron Neural Network	KDDCUP Arrhythmia Thyroid KDDCUP-Rev Yeast Abalone CTG Credit Covtype MMG Shuttle	F1-Score	0.94 0.47 0.57 0.91 0.33 0.55 0.66 0.64 0.86 0.60 0.93
Pant *et al 2020* [64]	(RNN) Recurrent Neural Network	Not clear	Not clear	Not clear
Tresp *et al 2021* [65]	unspecified	Omniglot CIFAR-FS MiniImageNet	Accuracy	0.961 0.681 0.645
Choe and Hong *2021* [66]	(AE) Autoencoder Neural Network + (CNN) Convolutional Neural Network	MNIST Fashion MNIST MVTec	ROC-AUC	0.977 0.927 0.777
Leckie and Ghafoori *2020* [67]	(AE) Autoencoder Neural Network	Variations of MNIST CIFAR-10 MobiAct (2nd version)	ROC-AUC	0.989 (average) 0.663 0.974
Mac Namee *et al 2020* [68]	(FNN) Feedforward Neural Network	Magic Gamma Telesacope Spambase Skin Segmentation Steel Plates Faults Image Segmentation Page Blocks Classification Statlog (Landsat Satellite) Waveform Database Generator	ROC-AUC	4.80% (average)
Yoon *et al 2020* [69]	(GNN) Graph Neural Network	Public Transport (PT) Computer Network (CN)	SumD ROC-AUC	10.2941 148.2091 0.9224 0.7202
Bower *et al 2019* [70]	(DRL) Deep Reinforcement Learning	Not available	Not available	Not available
Marecek and Akhriev *2019* [71]	(AE) Autoencoder Neural Network + (CNN) Convolutional Neural Network	CDnet	Recall Precision F-Measure	0.61160 0.57950 0.55863
Kumar *et al 2019* [72]	Unspecified (Deep) Neural Network	Cameras monitoring data	Not available	Not available
Patel and Perera *2019* [73]	(CNN) Convolutional Neural Network	Abnormal 1001 Caltech 256 UMDAA-02	ROC-AUC	0.956 0.981 0.810
Englund *et al 2019* [74]	(CNN) Convolutional Neural Network	CIFAR-10	ROC-AUC	0.87478

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

Iyengar and Oh *2019* [75]	(IRL) Inverse Reinforcement Learning	GeoLife GPS trajectory Taxi Service Trajectory (TST)	F1-Score	0.495 0.702
Tarokh *et al 2018* [76]	Unspecified (Deep) Neural Network	Not available	Not available	Not available
Xu *et al 2019* [77]	(CNN) Convolutional Neural Network	Omniglot	5-way 1-shot (%) 5-way 5-shot (%) 20-way 1-shot (%) 20-way 5-shot (%)	0.9909 ± 0.38 0.9965 ± 0.22 0.9705 ± 0.15 0.9937 ± 0.10
Kaur and Jain *2020* [78]	Unspecified (Deep) Neural Network	CIDDS-2017 NSL-KDD	Accuracy	0.8675 (average) 0.998
Tetko *et al 2019* [79]	(GAN) Generative Adversarial Network + (LSTM) Long Short-Term Memory (RNN)	SWaT / WADI / KDDCUP99	Precision Recall F1-Score	99.99 / 39.53 / 94.12 99.98 / 99.99 / 96.33 0.77 / 0.37 / 0.90
Jensen *et al 2019* [80]	(AE) Autoencoder Neural Network	Numenta Anomaly Benchmark (NAB) Electrocardiography(ECG)	PR-AUC ROC-AUC	0.923 0.976 0.676 0.777
Terejanu *et al 2018* [81]	(LSTM) Long Short-Term Memory (RNN)	Twitter 2013 Boston Marathon Event Twitter 2013 Superbowl Event Twitter 2013 OSCAR Event Twitter 2013 NBA AllStar Event Twitter Zimmerman Trial Event	Precision Recall F1-Score	0.400 0.545 0.641 0.667 0.609 0.571 0.474 0.568 0.537 0.708 0.471 0.507 0.602 0.595 0.655
Ahmed *et al 2019* [82]	(CNN) Convolutional Neural Network	Shuttle Pima ForestCover Ionosphere HTTP SMTP Mulcross Mammography	ROC-AUC	0.99 0.31 0.85 0.85 0.99 0.75 0.99 0.99
Turaga *et al 2017* [83]	(AE) Autoencoder Neural Network	Cardio / Ecoli / Lympho / Optdigits / Pendigits / Seismic / Thyroid / Waveform / Yeast	Accuracy	92.87 / 85.42 / 99.06 / 87.11 / 93.44 / 71.28 / 90.42 / 70.05 / 82.95
Tamukoh and Al aama *2020* [84]	(AE) Autoencoder Neural Network	CIFAR-10	F1-Score	Not clear to interpret value from the chart
Bohlouli *et al 2020* [85]	(MLP) Multi-Layer Perceptron Neural Network	WPBC Waveform Pima Ionosphere Annthyroid Parkinson	ROC-AUC (Not clear to interpret value from the charts)	0.98 0.98 0.91 0.95 0.95 1.00

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

Yang, *et al 2020* [86]	(CNN) Convolutional Neural Network	NSL-KDD UNSW-NB15 Credit Card Software Defect (JM1) Software Defect (PC5)	Accuracy Precision Recall F1-Score FPR G-Mean ROC-AUC	0.988 0.949 - - - 0.984 0.982 0.858 - - 0.991 0.925 0.832 0.830 0.930 0.988 0.953 0.845 0.613 0.780 0.014 0.021 0.0001 0.254 0.163 0.985 0.952 - 0.882 0.951 0.989 0.952 0.916 0.788 0.884
Alptekin and Kaplan *2020* [87]	(GAN) Generative Adversarial Network	KDDCUP99	Precision Recall Accuracy F1-Score	0.836 0.994 0.895 0.908
Song *et al 2020* [88]	Survey with multiple Techniques	Do not apply	Do not apply	Do not apply
Binsawad and Albahar *2020* [89]	(VAE) Variational Autoencoders (FNN) Feedforward Neural Network	NSL-KDD UNSW-NB15	Accuracy FPR TPR Precision F1-Score Accuracy FPR TPR Precision F1-Score	0.9701 0.9330 0.83 0.93 0.9542 0.9521 0.879 0.879 0.913 0.902 0.967 0.947 0.64 1.04 0.9586 0.9424 0.8820 0.8676 0.9096 0.8975
Alsalamn *et al 2021* [90]	(CNN) Convolutional Neural Network	MNIST CIFAR-10 CIFAR-100	Recall F1-Score FNR FPR	0.9756 0.9103 0.9221 0.9858 0.9494 0.9576 0.0877 0.4591 0.3180 0.0180 0.0363 0.0624
Sun *et al 2020* [91]	(SGPs) Sparse Gaussian Processes	Art Daily Jumpsup Art Daily Flatmiddle ec2 CPU Utilization 24ae8d ec2 CPU Utilization 825cc2 ec2 CPU Utilization ac20cd Grok Asg Anomaly Occupancy t4013 Speed t4013	F1-Score	0.9920 ± 0.00 0.9640 ± 0.01 0.9900 ± 0.01 0.9960 ± 0.01 0.9620 ± 0.01 0.9000 ± 0.01 0.8300 ± 0.01 0.8400 ± 0.00
Ueda *et al 2020* [92]	(AE) Autoencoder Neural Network	Annthyroid Cardiotocography InternetAds KDDCUP99 PageBlocks Pima SpamBase Waveform Wilt	ROC-AUC	0.867 0.846 0.828 0.992 0.914 0.713 0.791 0.746 0.895

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

Breckon *et al 2019* [93]	(CNN) Convolutional Neural Network	CIFAR-10 University Baggage Dataset (UBA) Full Firearm vs Operational Benign (FFOB)	ROC-AUC	0.731 (average) 0.940 (average) 0.903
Yang *et al 2019* [94]	Unspecified (Deep) Neural Network	MNIST Fashion-MNIST CIFAR-10	ROC-AUC	0.9423 (average) 0.9108 (average) 0.6927 (average)
Guo *et al 2019* [95]	(BP) Back-Propagation Neural Network	KPI1 / KPI2 / KPI3 / KPI4 / KPI5 / KPI6 / KPI7 / KPI8 / KPI9 / KPI10 / KPI11 / KPI12 / KPI13 / KPI14	Precision Recall F1-Score	0.8625 / 0.9950 / 1 / 0.9525 / 0.9975 / 0.8825 / 0.9487 / 0.9988 / 0.9938 / 0.9955 / 0.9738 / 0.9725 / 0.9800 / 0.9990 0.6141 / 0.8889 / 1 / 0.9525 / 0.7143 / 0.9769 / 0.9700 / 0.9955 / 0.8400 / 0.9862 / 0.7183 / 0.8571 / 0.9932 / 0.9985 0.7174 / 0.9390 / 1 / 0.9525 / 0.8325 / 0.9273 / 0.9592 / 0.9971 / 0.9104 / 0.9908 / 0.8267 / 0.9112 / 0.9865 / 0.9988
Kim *et al 2019* [96]	(LSTM) Long Short-Term Memory (RNN) (VAE) Variational Autoencoders	Kyoto-Honeypot UNSW-NB15 IDS2017	Precision Recall F1-Score MCC Precision Recall F1-Score MCC	1 1 1 1 1 1 1 1 1 1 - - 0.981 - - 0.901 - - 0.939 - - 0.19 - -
Om and Upasani *2018* [97]	(FMNN) Fuzzy Min-Max Neural Network	Disk Defect KDDCUP99	Accuracy	0.838 0.994
De Magistris *et al 2017* [98]	(AE) Autoencoder Neural Network	MNIST	Not available	Not available
Chawla *et al 2017* [99]	(AE) Autoencoder Neural Network	CIFAR-10	AUPRC AUROC P@10	0.6908 ± 0.0001 0.5576 ± 0.0005 0.5986 ± 0.0001
Li *et al 2021* [100]	(GNN) Graph Neural Network	Not available	Accuracy	94.78%
Liu *et al 2021* [28]	(GNN) Graph Neural Network	Yelp PubMed	AUC-ROC AUC-PR AUC-ROC AUC-PR	0.724 ± 0.012 0.175 ± 0.011 0.761 ± 0.014 0.485 ± 0.010

TABLE 6. *(Continued.)* **Datasets and Metrics compiled from the researched articles.**

		Reddit	AUC-ROC AUC-PR	0.842 ± 0.011 0.395 ± 0.009
Jin *et al 2021* [101]	(VAE) Variational Autoencoders (RNN) Recurrent Neural Network	Open μ PMU Power Network	AUC-ROC AUC-PR F1-Score	0.814 0.310 0.367
Adeli *et al 2021* [102]	(GAN) Generative Adversarial Network	MNIST Caltech-256	AUC-ROC F1-Score	0.95 0.93
Kim *et al 2019* [103]	Survey with multiple Techniques	Do not apply	Do not apply	Do not apply
Del Ser *et al 2021* [104]	Spiking Neural Network	The Yahoo Anomaly Dataset	F1-Score	0.427 0.234 0.369 0.324 0.340 0.310
Chen *et al 2021* [105]	(GNN) Graph Neural Network	Reddit Wiki Alpha Amazon	Accuracy	0.746 0.762 0.907 0.810
Müller *et al 2021* [31]	Survey with multiple Techniques	Do not apply	Do not apply	Do not apply
Bauchy *et al 2021* [106]	Unspecified (Deep) Neural Network	Delta Elevators Red wine Airfoil noise Qsar fish toxicity Boston Housing California Housing Ailerons Abalone UCI concrete Real estate	Accuracy	0.711 0.362 0.931 0.725 0.909 0.842 0.841 0.610 0.918 0.752
Hu *et al 2019* [107]	Unspecified (Deep) Neural Network	MNIST RGB-D	Accuracy / Precision / Recall	0.992/0.997/0.987 0.951/0.931/0.974

for finding a small number of outliers that are the most visible from their individual perspectives, as shown in [106]. Moreover, compared to employing a single detector, using an ensemble of weak detectors minimizes the potential of bias during outlier detection, mainly dealing with noisy datasets.

Generative/reconstruction model-based approaches for OOD detection have an advantage because they do not require any labels for training [53].

Deep convolutional neural networks are widely used in the field of computer vision, producing state-of-the-art performance in many classification, action detection and consequently anomaly detection tasks.

Generative Model Base Approach and autoencoders Base models require no labels for training. Anomaly detection performance degrades less due changes intraclass variance and diferent input complexity.

E. WHAT ARE THE CURRENT CHALLENGES OF OUTLIER DETECTION TECHNIQUES?

This research question aims to identify the main difficulties faced by scientists in detecting anomalies using neural networks, will be addressed. As a fundamental point of this review, the intention is to map some research gaps, in order to solve them in the future.

Anomaly detection is a difficult problem to solve in general and for that reason most of the techniques in the literature tend to solve a specific case of the general problem, based on the type of application, type of input data and model, availability of labels for the training and testing data and also the types of anomalies. A particular difficult problem is when the abnormal examples in the dataset tend to disguise as normal data. [88]

The study made by [114] indicates that methods that leverage descriptors of pre-trained networks perform better than all other approaches and deep-learning-based generative models show considerable room for improvement.

Deep detection models can learn abnormalities beyond given anomaly examples scope. Therefore, it would be necessary to understand and explore the extent of the generalizability and develop models to improve the accuracy [115], [116], [117], [118].

Big Data Normality Learning is a challenging learning task to obtain sufficient anomaly labeled data. The goal is to transfer pre-trained representations to act unsupervised on unknown data.

Several anomaly detection methods address on isolated anomalies. However, contextual and collective ones are significantly less explored.

Deep learning has superior capability in capturing the complex temporal/spatial dependence and learning representations of a set of unordered data points. It is essential to explore whether deep learning could also detect such complex anomalies better. For example, one can explore new neural network layers or new loss functions.

Without proper regularization, reconstruction-based methods, as GAN, can easily become overfitted, resulting in low performance [57].

F. REVIEW LIMITATIONS

This research only focuses on journal and conference papers related to outlier detection using neural networks. The protocol excluded several papers at the initial review step. All papers match the research criteria and this review excludes approach only for specific purpose as shown in Table 3. Furthermore, the same principle applies to quality evaluation, as shown in Table 4.

VI. CONCLUSION

The protocol reaches 1422 papers as shown in Table 5. After applying inclusion and exclusion criteria detailed in Table 3, and quality assessment described in section II-D there were 76 papers left for the review as shown in Section V-A.

This study reviews anomaly detection using neural networks techniques. The main goal is look three perspectives: What kinds of Neural Networks are used to outlier detection, what are neural networks strengths for outlier detection and what are the current challenges of outlier detection techniques.

A. FUTURE WORKS

There are some fascinating new research applications and issue contexts where there may be significant room to develop deep detection techniques. For example, the majority of shallow and deep models for anomaly identification assume that data anomalies are independently and uniformly distributed. However, in reality, these assumptions are not always accurate, and it is an exciting gap to investigate.

The manuscript will be enriched with publications from 2022 onward, and additional research questions will be included; for example, what are data types used? What is the anomaly detection technique used within each data type? Also, How is RNN formulated to detect deviations in serial data? How is CNN used to extract features from array data? Or how are attention models used to learn patterns in array data?

The data types are fundamental because they can directly influence the choice of the most appropriate technique. Include discussions about the technical approaches that could be performed. At last, a discussion of the strategies and patterns can be valuable in providing deep analysis and investigation of the topic.

CONFLICT OF INTEREST

The authors have no conflicts of interest to declare that are relevant to the content of this article.

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, Jul. 2009.
[2] B. Kitchenham, "Procedure for undertaking systematic reviews," Comput. Sci. Dept., Keele Univ. (TRISE) Nat. ICT Aust., Sydney, NSW, Australia, Tech. Rep. 33, 2004.
[3] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," EBSE, Goyang-Si, South Korea, Tech. Rep. Version 2.3, 2007.
[4] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021.
[5] F. J. Anscombe, "Rejection of outliers," *Technometrics*, vol. 2, no. 2, pp. 123–146, May 1960.
[6] F. E. Grubbs, "Procedures for detecting outlying observations in samples," *Technometrics*, vol. 11, no. 1, pp. 1–21, 1969.
[7] D. M. Hawkins, *Identification of Outliers*, vol. 11. London, U.K.: Chapman & Hall, 1980.
[8] V. Barnett and T. Lewis, "Outliers in statistical data," in *Wiley Series in Probability and Mathematical Statistics* (Applied Probability and Statistics). Chichester, U.K.: Wiley, 1984.
[9] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," *ACM SIGMOD Rec.*, vol. 29, no. 2, pp. 93–104, 2000.
[10] M.-F. Jiang, S.-S. Tseng, and C.-M. Su, "Two-phase clustering process for outliers detection," *Pattern Recognit. Lett.*, vol. 22, nos. 6–7, pp. 691–700, 2001.
[11] S. Hawkins, H. He, G. Williams, and R. Baxter, "Outlier detection using replicator neural networks," in *Proc. Int. Conf. Data Warehousing Knowl. Discovery*. Berlin, Germany: Springer, 2002, pp. 170–180.
[12] T. Hu and S. Y. Sung, "Detecting pattern-based outliers," *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 3059–3068, Dec. 2003.
[13] C. C. Aggarwal and P. S. Yu, "An effective and efficient algorithm for high-dimensional outlier detection," *VLDB J.*, vol. 14, no. 2, pp. 211–221, 2005.
[14] S. Sadik and L. Gruenwald, "Online outlier detection for data streams," in *Proc. 15th Symp. Int. Database Eng. Appl. (IDEAS)*, New York, NY, USA, 2011, pp. 88–96.
[15] C. C. Aggarwal and P. S. Yu, "Outlier detection for high dimensional data," in *Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD)*, 2001, pp. 37–46.
[16] E. M. Knorr and R. T. Ng, "Finding intensional knowledge of distance-based outliers," in *Proc. VLDB*, vol. 99, 1999, pp. 211–222.
[17] L. N. D. Castro and D. G. Ferrari, "Introdução à mineração de dados: Conceitos básicos, algoritmos e aplicações," *São Paulo: Saraiva*, vol. 5, pp. 1–376, Mar. 2016.
[18] N. Görnitz, M. Kloft, K. Rieck, and U. Brefeld, "Toward supervised anomaly detection," *J. Artif. Intell. Res.*, vol. 46, pp. 235–262, Jan. 2013.
[19] O. Chapelle, B. Scholkopf, and A. Zien, "Semi-supervised learning (Chapelle, O. et al., Eds.; 2006) [Book reviews]," *IEEE Trans. Neural Netw.*, vol. 20, no. 3, p. 542, Mar. 2009.
[20] T. Schlegl, P. Seeböck, 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.* Cham, Switzerland: Springer, 2017, pp. 146–157.
[21] M. Valença, *Aplicando Redes Neurais: UM GUIA COMPLETO*. Olinda: Meuser Valença, 2016.
[22] N. K. Manaswi, N. K. Manaswi, and S. John, *Deep Learning With Applications Using Python*. Berkeley, CA, USA: Apress, 2018.
[23] D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," 2014, *arXiv:1312.6114*.
[24] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," Assoc. Comput. Machinery, New York, NY, USA, Tech. Rep. ACM 63.11, 2014.
[25] L. Deng and D. Yu, "Deep learning: Methods and applications," *Found. Trends Signal Process.*, vol. 7, nos. 3–4, pp. 197–387, Jun. 2014.
[26] B. Juba and H. S. Le, "Precision-recall versus accuracy and the role of large data sets," in *Proc. AAAI Conf. Artif. Intell.*, 2019, vol. 33, no. 1, pp. 4039–4048.
[27] Y. Sasaki, "The truth of the F-measure," *Teach Tutor Mater*, vol. 1, no. 5, pp. 1–5, 2007.

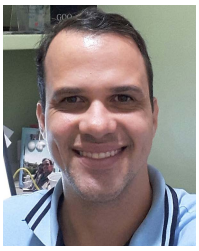
[28] K. Ding, Q. Zhou, H. Tong, and H. Liu, "Few-shot network anomaly detection via cross-network meta-learning," in *Proc. Web Conf.*, Ljubljana, Slovenia, Apr. 2021, pp. 2448–2456.
[29] B. J. Beula Rani and L. Sumathi M. E, "Survey on applying GAN for anomaly detection," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2020, pp. 1–5.
[30] 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. 2021.
[31] 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.
[32] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016.
[33] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.
[34] J. Kauffmann, K.-R. Müller, and G. Montavon, "Towards explaining anomalies: A deep Taylor decomposition of one-class models," *Pattern Recognit.*, vol. 101, May 2020, Art. no. 107198.
[35] J. Wang, W. Huang, S. Wang, P. Dai, and Q. Li, "LRGAN: Visual anomaly detection using GAN with locality-preferred recoding," *J. Vis. Commun. Image Represent.*, vol. 79, Aug. 2021, Art. no. 103201.
[36] Z. Wang, Z. Chen, J. Ni, H. Liu, H. Chen, and J. Tang, "Multi-scale one-class recurrent neural networks for discrete event sequence anomaly detection," in *Proc. 27th ACM SIGKDD Conf. Knowl. Discovery Data Mining*, Aug. 2021, pp. 3726–3734.
[37] T. Zhao, C. Deng, K. Yu, T. Jiang, D. Wang, and M. Jiang, "Error-bounded graph anomaly loss for GNNs," in *Proc. 29th ACM Int. Conf. Inf. Knowl. Manage.*, Oct. 2020, pp. 1873–1882.
[38] Q. Chen, A. Zhang, T. Huang, Q. He, and Y. Song, "Imbalanced dataset-based echo state networks for anomaly detection," *Neural Comput. Appl.*, vol. 32, no. 8, pp. 3685–3694, Apr. 2020.
[39] D. Chakraborty, V. Narayanan, and A. Ghosh, "Integration of deep feature extraction and ensemble learning for outlier detection," *Pattern Recognit.*, vol. 89, pp. 161–171, May 2019.
[40] X. Zhang, J. Mu, X. Zhang, H. Liu, L. Zong, and Y. Li, "Deep anomaly detection with self-supervised learning and adversarial training," *Pattern Recognit.*, vol. 121, Jan. 2022, Art. no. 108234.
[41] R. Wang, K. Nie, Y.-J. Chang, X. Gong, T. Wang, Y. Yang, and B. Long, "Deep learning for anomaly detection," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining* Aug. 2020, pp. 3569–3570.
[42] L. Ahrens, J. Ahrens, and H. D. Schotten, "A machine-learning phase classification scheme for anomaly detection in signals with periodic characteristics," *EURASIP J. Adv. Signal Process.*, vol. 2019, no. 1, p. 27, Dec. 2019.
[43] T. Chen, X. Liu, B. Xia, W. Wang, and Y. Lai, "Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder," *IEEE Access*, vol. 8, pp. 47072–47081, 2020.
[44] N. AlDahoul, H. Abdul Karim, and A. S. Ba Wazir, "Model fusion of deep neural networks for anomaly detection," *J. Big Data*, vol. 8, no. 1, p. 106, Dec. 2021.
[45] A. S. Hashmi and T. Ahmad, "GP-ELM-RNN: Garson-pruned extreme learning machine based replicator neural network for anomaly detection," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 5, pp. 1768–1774, May 2022.
[46] A.-A. Papadopoulos, M. R. Rajati, N. Shaikh, and J. Wang, "Outlier exposure with confidence control for out-of-distribution detection," *Neurocomputing*, vol. 441, pp. 138–150, Jun. 2021.
[47] H. Cevikalp, B. Uzun, O. Köpüklü, and G. Ozturk, "Deep compact polyhedral conic classifier for open and closed set recognition," *Pattern Recognit.*, vol. 119, Nov. 2021, Art. no. 108080.
[48] H. Dai, J. Cao, T. Wang, M. Deng, and Z. Yang, "Multilayer one-class extreme learning machine," *Neural Netw.*, vol. 115, pp. 11–22, Jul. 2019.
[49] G. S. Chadha, I. Islam, A. Schwung, and S. X. Ding, "Deep convolutional clustering-based time series anomaly detection," *Sensors*, vol. 21, no. 16, p. 5488, Aug. 2021.
[50] G. García González, P. Casas, A. Fernández, and G. Gómez, "On the usage of generative models for network anomaly detection in multivariate time-series," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 48, no. 4, pp. 49–52, May 2021.
[51] Y. Chen, H. Zhang, Y. Wang, Y. Yang, X. Zhou, and Q. M. J. Wu, "MAMA Net: Multi-scale attention memory autoencoder network for anomaly detection," *IEEE Trans. Med. Imag.*, vol. 40, no. 3, pp. 1032–1041, Mar. 2021.
[52] P. Zhao, X. Chang, and M. Wang, "A novel multivariate time-series anomaly detection approach using an unsupervised deep neural network," *IEEE Access*, vol. 9, pp. 109025–109041, 2021.
[53] J. Lee, M. Umar Karim Khan, and C.-M. Kyung, "Hybrid discriminator with correlative autoencoder for anomaly detection," *IEEE Access*, vol. 9, pp. 49098–49109, 2021.
[54] H. Sarvari, C. Domeniconi, B. Prenkaj, and G. Stilo, "Unsupervised boosting-based autoencoder ensembles for outlier detection," in *Advances in Knowledge Discovery and Data Mining* (Lecture Notes in Computer Science), vol. 12712, K. Karlapalem, H. Cheng, N. Ramakrishnan, R. K. Agrawal, P. K. Reddy, J. Srivastava, and T. Chakraborty, Eds. Cham, Switzerland: Springer, 2021, pp. 91–103.
[55] L. Deng, X. Chen, Y. Zhao, and K. Zheng, "HIFI: Anomaly detection for multivariate time series with high-order feature interactions," in *Database Systems for Advanced Applications* (Lecture Notes in Computer Science), vol. 12681, C. S. Jensen, E.-P. Lim, D.-N. Yang, W.-C. Lee, V. S. Tseng, V. Kalogeraki, J.-W. Huang, and C.-Y. Shen, Eds. Cham, Switzerland: Springer, 2021, pp. 641–649.
[56] P. Sperl, J.-P. Schulze, and K. Böttinger, "Activation anomaly analysis," in *Machine Learning and Knowledge Discovery in Databases* (Lecture Notes in Computer Science), vol. 12458, F. Hutter, K. Kersting, J. Lijffijt, and I. Valera, Eds. Cham, Switzerland: Springer, 2021, pp. 69–84.
[57] 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)*, Atlanta, GA, USA, Dec. 2020, pp. 33–43.
[58] M. A. Bashar and R. Nayak, "TAnoGAN: Time series anomaly detection with generative adversarial networks," in *Proc. IEEE Symp. Comput. Intell. (SSCI)*, Canberra, ACT, Australia, Dec. 2020, pp. 1778–1785.
[59] S. Aburakhia, T. Tayeh, R. Myers, and A. Shami, "A transfer learning framework for anomaly detection using model of normality," in *Proc. 11th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Vancouver, BC, Canada, Nov. 2020, pp. 0055–0061.
[60] G. Kwon, M. Prabhushankar, D. Temel, and G. AlRegib, "Novelty detection through model-based characterization of neural networks," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Abu Dhabi, United Arab Emirates, Oct. 2020, pp. 3179–3183.
[61] J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, "USAD: Unsupervised anomaly detection on multivariate time series," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2020, pp. 3395–3404.
[62] T. Ergen and S. S. Kozat, "Unsupervised anomaly detection with LSTM neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 8, pp. 3127–3141, Aug. 2020.
[63] T. Pimentel, M. Monteiro, A. Veloso, and N. Ziviani, "Deep active learning for anomaly detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Glasgow, U.K., Jul. 2020, pp. 1–8.
[64] T. Nolle, A. Seeliger, N. Thoma, and M. Mühlhäuser, "DeepAlign: Alignment-based process anomaly correction using recurrent neural networks," in *Advanced Information Systems Engineering* (Lecture Notes in Computer Science), vol. 12127, S. Dustdar, E. Yu, C. Salinesi, D. Rieu, and V. Pant, Eds. Cham, Switzerland: Springer, 2020, pp. 319–333.
[65] A. Frikha, D. Krompass, and V. Tresp, "ARCADe: A rapid continual anomaly detector," in *Proc. 25th Int. Conf. Pattern Recognit. (ICPR)*, Milan, Italy, Jan. 2021, pp. 10449–10456.
[66] E. Hong and Y. Choe, "Latent feature decentralization loss for one-class anomaly detection," *IEEE Access*, vol. 8, pp. 165658–165669, 2020.
[67] Z. Ghafoori and C. Leckie, "Deep multi-sphere support vector data description," in *Proc. SIAM Int. Conf. Data Mining*, 2020, pp. 109–117.
[68] M. Hossein Zadeh Bazargani and B. Mac Namee, "The elliptical basis function data descriptor (EBFDD) network: A one-class classification approach to anomaly detection," in *Machine Learning and Knowledge Discovery in Databases* (Lecture Notes in Computer Science), vol. 11906, U. Brefeld, E. Fromont, A. Hotho, A. Knobbe, M. Maathuis, and C. Robardet, Eds. Cham, Switzerland: Springer, 2020, pp. 107–123.
[69] J. Lee, H. Bae, and S. Yoon, "Anomaly detection by learning dynamics from a graph," *IEEE Access*, vol. 8, pp. 64356–64365, 2020.
[70] P. M. Dassanayake, A. Anjum, W. Manning, and C. Bower, "A deep reinforcement learning based homeostatic system for unmanned position control," in *Proc. 6th IEEE/ACM Int. Conf. Big Data Comput., Appl. Technol. (BDCAT)*, Auckland, New Zealand, Dec. 2019, pp. 127–136.

[71] A. Akhriev and J. Marecek, "Deep autoencoders with value-at-risk thresholding for unsupervised anomaly detection," in *Proc. IEEE Int. Symp. Multimedia (ISM)*, San Diego, CA, USA, Dec. 2019, pp. 208–2083.
[72] J. Gowthamy, S. K. Swamy, M. Kumar, and M. Kumar, "Computation of person re-identification using self-learning anomaly detection framework in deep-learning," *Int. J. Innov. Technol. Exploring Eng.*, vol. 9, no. 1, pp. 1106–1109, Nov. 2019.
[73] 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.
[74] J. Henriksson, C. Berger, M. Borg, L. Tornberg, S. R. Sathyamoorthy, and C. Englund, "Performance analysis of out-of-distribution detection on various trained neural networks," in *Proc. 45th Euromicro Conf. Softw. Eng. Adv. Appl. (SEAA)*, Kallithea-Chalkidiki, Greece, Aug. 2019, pp. 113–120.
[75] M.-H. Oh and G. Iyengar, "Sequential anomaly detection using inverse reinforcement learning," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Anchorage, AK USA, Jul. 2019, pp. 1480–1490.
[76] T. Banerjee, G. Whipps, P. Gurram, and V. Tarokh, "Cyclostationary statistical models and algorithms for anomaly detection using multi-modal data," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Anaheim, CA, USA, Nov. 2018, pp. 126–130.
[77] J. Shi, J. Xu, Y. Yao, and B. Xu, "Concept learning through deep reinforcement learning with memory-augmented neural networks," *Neural Netw.*, vol. 110, pp. 47–54, Feb. 2019.
[78] M. Jain and G. Kaur, "A study of feature reduction techniques and classification for network anomaly detection," *J. Comput. Inf. Technol.*, vol. 27, no. 4, pp. 1–16, Jun. 2020.
[79] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S.-K. Ng, "MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," in *Artificial Neural Networks and Machine Learning–ICANN 2019: Text and Time Series* (Lecture Notes in Computer Science), vol. 11730, I. V. Tetko, V. Kurková, P. Karpov, and F. Theis, Eds. Cham, Switzerland: Springer, 2019, pp. 703–716.
[80] T. Kieu, B. Yang, C. Guo, and C. S. Jensen, "Outlier detection for time series with recurrent autoencoder ensembles," in *Proc. 28th Int. Joint Conf. Artif. Intell.*, Macao, China, Aug. 2019, pp. 2725–2732.
[81] C. Chen, X. Lin, and G. Terejanu, "An approximate Bayesian long short-term memory algorithm for outlier detection," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Beijing, China, Aug. 2018, pp. 201–206.
[82] 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, 2018.
[83] J. Chen, S. Sathe, C. Aggarwal, and D. Turaga, *Outlier Detection With Autoencoder Ensembles*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2017, pp. 90–98.
[84] O. Al aama and H. Tamukoh, "Training autoencoder using three different reversed color models for anomaly detection," *J. Robot., Netw. Artif. Life*, vol. 7, no. 1, p. 35, 2020.
[85] R. Kiani, A. Keshavarzi, and M. Bohlouli, "Detection of thin boundaries between different types of anomalies in outlier detection using enhanced neural networks," *Appl. Artif. Intell.*, vol. 34, no. 5, pp. 345–377, Apr. 2020.
[86] X. Liu, X. Di, Q. Ding, W. Liu, H. Qi, J. Li, and H. Yang, "NADS-RA: Network anomaly detection scheme based on feature representation and data augmentation," *IEEE Access*, vol. 8, pp. 214781–214800, 2020.
[87] M. O. Kaplan and S. E. Alptekin, "An improved BiGAN based approach for anomaly detection," *Proc. Comput. Sci.*, vol. 176, pp. 185–194, Jan. 2020.
[88] S. Bulusu, B. Kailkhura, B. Li, P. K. Varshney, and D. Song, "Anomalous example detection in deep learning: A survey," *IEEE Access*, vol. 8, pp. 132330–132347, 2020.
[89] M. A. Albahar and M. Binsawad, "Deep autoencoders and feedforward networks based on a new regularization for anomaly detection," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jul. 2020.
[90] F. Alharbi, K. El Hindi, S. Al Ahmadi, and H. Alsalamn, "Convolutional neural network-based discriminator for outlier detection," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–13, Mar. 2021.
[91] M. Gu, J. Fei, and S. Sun, "Online anomaly detection with sparse Gaussian processes," *Neurocomputing*, vol. 403, pp. 383–399, Aug. 2020.
[92] T. Iwata, M. Toyoda, S. Tora, and N. Ueda, "Anomaly detection with inexact labels," *Mach. Learn.*, vol. 109, no. 8, pp. 1617–1633, Aug. 2020.
[93] S. Akcay, 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.
[94] P. Schlachter, Y. Liao, and B. Yang, "Deep one-class classification using intra-class splitting," in *Proc. IEEE Data Sci. Workshop (DSW)*, Minneapolis, MN, USA, Jun. 2019, pp. 100–104.
[95] Y. Zhang, Y. Zhu, X. Li, X. Wang, and X. Guo, "Anomaly detection based on mining six local data features and BP neural network," *Symmetry*, vol. 11, no. 4, p. 571, Apr. 2019.
[96] R. K. Malaiya, D. Kwon, S. C. Suh, H. Kim, I. Kim, and J. Kim, "An empirical evaluation of deep learning for network anomaly detection," *IEEE Access*, vol. 7, pp. 140806–140817, 2019.
[97] N. Upasani and H. Om, "Optimized fuzzy min-max neural network: An efficient approach for supervised outlier detection," *Neural Netw. World*, vol. 28, no. 4, pp. 285–303, 2018.
[98] A. Munawar, P. Vinayavekhin, and G. De Magistris, "Limiting the reconstruction capability of generative neural network using negative learning," in *Proc. IEEE 27th Int. Workshop Mach. Learn. Signal Process. (MLSP)*, Tokyo, Japan, Sep. 2017, pp. 1–6.
[99] R. Chalapathy, A. K. Menon, and S. Chawla, "Robust, deep and inductive anomaly detection," in *Machine Learning and Knowledge Discovery in Databases* (Lecture Notes in Computer Science), vol. 10534, M. Ceci, J. Hollmén, L. Todorovski, C. Vens, and S. Dzeroski, Eds. Cham: Springer, 2017, pp. 36–51.
[100] Y. Ji, J. Wang, S. Li, Y. Li, S. Lin, and X. Li, "An anomaly event detection method based on GNN algorithm for multi-data sources," in *Proc. 3rd ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, Hong Kong, May 2021, pp. 91–96.
[101] L. Li, J. Yan, H. Wang, and Y. Jin, "Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 3, pp. 1177–1191, Mar. 2021.
[102] M. Sabokrou, M. Fathy, G. Zhao, and E. Adeli, "Deep end-to-end one-class classifier," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 2, pp. 675–684, Feb. 2021.
[103] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Comput.*, vol. 22, pp. 949–961, Jan. 2019.
[104] P. S. Maciąg, M. Kryszkiewicz, R. Bembenik, J. L. Lobo, and J. Del Ser, "Unsupervised anomaly detection in stream data with online evolving spiking neural networks," *Neural Netw.*, vol. 139, pp. 118–139, Jul. 2021.
[105] Y. Wang, J. Zhang, S. Guo, H. Yin, C. Li, and H. Chen, "Decoupling representation learning and classification for GNN-based anomaly detection," in *Proc. 44th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr.*, Jul. 2021, pp. 1239–1248.
[106] B. Ouyang, Y. Song, Y. Li, G. Sant, and M. Bauchy, "EBOD: An ensemble-based outlier detection algorithm for noisy datasets," *Knowl.-Based Syst.*, vol. 231, Nov. 2021, Art. no. 107400.
[107] Y. Li, N. Liu, J. Li, M. Du, and X. Hu, "Deep structured cross-modal anomaly detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Budapest, Hungary, Jul. 2019, pp. 1–8.
[108] A. Krizhevsky and G. Hinton, "Learning multiple layers of features from tiny images," Univ. Toronto, Toronto, ON, Canada, Tech. Rep., 2009.
[109] L. Deng, "The MNIST database of handwritten digit images for machine learning research," *IEEE Signal Process. Mag.*, vol. 29, no. 6, pp. 141–142, Nov. 2012.
[110] A. C. Ian Goodfellow and Y. Bengio, "Deep learning," in *The Reference Book for Deep Learning Models*. Cambridge, MA, USA: MIT Press, 2016.
[111] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 25, 2012, pp. 1097–1105.
[112] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.
[113] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.
[114] P. Bergmann, K. Batzner, M. Fauser, D. Sattlegger, and C. Steger, "The MVTec anomaly detection dataset: A comprehensive real-world dataset for unsupervised anomaly detection," *Int. J. Comput. Vis.*, vol. 129, pp. 1038–1059, Apr. 2021.
[115] G. Pang, A. van den Hengel, C. Shen, and L. Cao, "Toward deep supervised anomaly detection: Reinforcement learning from partially labeled anomaly data," in *Proc. 27th ACM SIGKDD Conf. Knowl. Discovery Data Mining*, 2021, pp. 1298–1308.

[116] G. Pang, C. Shen, H. Jin, and A. van den Hengel, "Deep weakly-supervised anomaly detection," 2019, *arXiv:1910.13601*.
[117] G. Pang, C. Shen, and A. van den Hengel, "Deep anomaly detection with deviation networks," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2019, pp. 353–362.
[118] L. Ruff, R. A. Vandermeulen, N. Görnitz, A. Binder, E. Müller, K.-R. Müller, and M. Kloft, "Deep semi-supervised anomaly detection," 2019, *arXiv:1906.02694*.

JOSÉ EDSON DE ALBUQUERQUE FILHO received the B.Sc. and M.Sc. degrees in computer science from the Federal University of Pernambuco, Recife, Brazil, in 2002 and 2003, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, University of Pernambuco. He was a Professor with the Faculdade Maurício de Nassau and a Software Engineer Coordinator with the Data Process Federal Bureau (SERPRO), Brazil. He is a Senior System Analyst with the Business Intelligence Division, Pernambuco Prosecution Office. His research interests include machine learning, neural networks, and anomaly detection.

LAISLLA C. P. BRANDÃO received the B.Sc. degree in electrical and electronic engineering from the Federal University of Pernambuco, Recife, Brazil, in 2011. She is currently pursuing the M.Sc. degree with the Department of Computer Engineering, University of Pernambuco, Recife. Her research interests include artificial intelligence and the design and analysis of machine learning algorithms for anomaly detection and the prediction of anomalies applied to the welding process of the automotive industry.



BRUNO JOSÉ TORRES FERNANDES (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science from the Federal University of Pernambuco, Recife, Brazil, in 2007, 2009, and 2013, respectively. He is currently an Associate Professor with the University of Pernambuco, where he received the title of Livre-Docente, in 2017. He is also a CNPq Productivity Fellow of technological development, the Coordinator with the Computer Vision Laboratory, Instituto de Inovação Tecnológica (IIT -UPE), and the Head of the Pattern Recognition and Digital Image Processing Research Group, UPE. His research interests include machine learning, computer vision, image processing, and neural networks. He was a recipient of awards, including the 2008 Google Academic Prize as the Top M.Sc. Student in the Federal University of Pernambuco and the Science and Technology Award for Outstanding Research in the Polytechnic School, University of Pernambuco, in 2011 and 2017.

ALEXANDRE M. A. MACIEL received the Ph.D. degree in computer science from the Federal University of Pernambuco, in 2012.

He was the Chief Scientist of the Technological Innovation Institute, UPE (IIT/UPE), a member of the Innovation Chamber of Fundação de Amparo à Pesquisa do Estado de Pernambuco (FACEPE) (Foundation of Support for Science and Technology of the State of Pernambuco), and a Visiting Researcher at the State Agency for Information Technology (ATI). He is an Associate Professor of computer engineering and the Coordinator of the Data Science and Analytics Course with the University of Pernambuco (UPE). Currently, he is the General Manager of Innovation Environments with the Secretary of Science, Technology, and Innovation of Pernambuco State.

Dr. Maciel received the Santander Science and Innovation Award in the Information Technology and Education Category.