JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 06 Issue 01
2023
Review Article
https://doi.org/10.56979/601/2023

A Comprehensive Review and Analysis of Anomaly Detection

Syeda Mariyum Nizami[1*], Ramesha Rehman[1], and Khalid Masood[1]

[1]Lahore Garrison University, Lahore, 54000, Pakistan.
*Corresponding Author: Syeda Mariyum Nizami. Email: mariyum.nizami@lgu.edu.pk

Received: August 18, 2023 **Accepted:** December 01, 2023 **Published:** December 05, 2023

Abstract: This research work emphasizes on the challenges and issues faced by a researcher while working on anomaly detection using deep learning. The motivation behind this research is to highlight the initial challenges and complexities encountered at the commencement of anomaly detection. The primary hurdle involves the precise identification and categorization of anomalies, with this paper expounding on various anomaly types and their distinctive characteristics. Another challenge arises in the analytical process of discerning and selecting the most optimal model, considering their varying levels of accuracy. So to make this task simpler the research elucidates various deep learning models. Subsequently, it conducts a comprehensive review of the work undertaken by different researchers in the realm of anomaly detection, comparing their learnings and outputs. And the most accurate model is suggested. [37].

Keywords: Anomaly Detection; Deep Learning ; One-class Classification; Generative Cooperative Learning ; CNN.

1. Introduction

The background of anomaly detection is rooted in various disciplines and has evolved over time. Anomaly detection has historical roots in quality control processes in manufacturing, where deviations from expected specifications were identified to maintain product quality [24]. Statistical methods, such as control charts developed by Walter A. Shewhart in the 1920s, were early tools for detecting anomalies by monitoring variations in production processes. In the mid-20th century, time series analysis techniques emerged, and researchers began applying statistical methods to detect anomalies in sequences of data, such as financial transactions or sensor readings. In the early 2000s, the isolation forest algorithm was introduced, providing a scalable and efficient method for isolating anomalies by leveraging the characteristics of random forests. Anomaly detection shifted towards machine learning and data mining approaches, particularly unsupervised learning techniques, where models are trained on normal data and anomalies are identified as deviations from the learned patterns [25]. Clustering methods, such as k-means, were adapted for anomaly detection, where anomalies were treated as data points that did not fit well into any cluster. Anomaly detection has found applications in diverse industries, including finance, cybersecurity, healthcare, and industrial operations, reflecting its broad utility in identifying irregularities and potential issues within complex systems. The background of anomaly detection is characterized by a continuous evolution, driven by advancements in statistical methods, machine learning, and deep learning [26]. As technology continues to progress, so does the sophistication and effectiveness of anomaly detection techniques of research.

2. Literature Review

The below Table 1, shows the comparison of deep learning approaches for anomaly detection used in the recent studies

Table 1. Comparison table of Deep Learning approaches for Anomaly detection

S. no	Ref.	Model	Dataset	Strength	Strength/Drawbacks
1.	Quatrini et al., 2020[1]	Decision Trees	Real-World Dataset	Extensive training times are necessary for model training.	a well-known anomaly detector, is employed, particularly suited for industrial data.
2.	Liu et al., 2020 [2]	Long Short-term memory	Synthetic data and public domain data	The LSTM and auto-encoder (AE) based models demonstrate superior performance compared to state-of-the-art models. [59]	In an autoencoder-based approach, the presence of uncommon regularities and distort the learned feature representations.
3.	Ganokratanaa et al., 2020 [3]	Convolutional Neural Networks	CUHK Avenue	The proposed approach demands more computation power due to its utilization of Encode and Decode Recurrent Neural Network as its architecture.	Through the implementation of Edge Wrapping, the proposed approach enhances Additionally, it autonomously learns normal samples without the need for modifying any settings.
4.	Mehta et al., 2020 [4]			The proposed model can be commercially deployed on any GPU-based system for the reliable identification of fire	The proposed anomaly detection system is specifically designed for fire detection and has potential for improvement and diversification.
5.	Ilyas et al., 2021[5]		PETS 2009	The work proposes the incorporation of a manually crafted feature to capture high-level changes at the frame level, and the combination model yields improved outcomes.	The proposed model is no t suitable for pixel-level feature extraction.
6.	Liu et al., 2020[6]	Support Vector Machine	Synthetic data and public domain data	The model is trained using a one-class support vector machine (1-SVM) approach, and its performance, along with the algorithms.	The model is trained using a one-class support vector machine (1-SVM) approach, and its performance, along with the algorithms, is assessed using real data sourced from Colorado Water Watch.
7.	Aziz et al., 2021[7]		UMN datasets	The proposed technique has the capability to reduce false motion anomaly detection and localization alarms.	There are temporal and spatial instances when the proposed paradigm is inappropriate. When dealing with datasets that exhibit complex distributions within the normal class, the one-class

					SVM model is not the best fit.
8.	Alfie et al., 2021[8]	Generative adversarial network	Real-world data (Hajj)	For spatial and temporal circumstances, the suggested paradigm is inappropriate. For datasets with complex distributions inside the normal class, the one-class SVM model is not a good fit.	To increase the model's accuracy, more improvements are needed, especially when using large-scale crowd datasets.
9.	Barua et al., 2020[9]	Hierarchical Temporal Memory	Benign IoT traffic	The work presents a novel method for real-time anomaly identification that does not require human involvement. It uses hierarchical temporal memory (HTM) in conjunction with ongoing unsupervised learning.	Because the input data for unsupervised learning is unknown and not pre-classified, the results are less reliable.
10.	Zhao et el., 2020[10]	Attention networks	SMAP MSL, TSA,SMAP [39]	The foundation of the research is the dynamic handling of several time series through the use of parallel graph attention layers.	An important constraint of the research is its incapacity to ascertain the topological configuration among the sensors., particularly in densely populated and highly connected sensor environments, which may result in overlooking large relational data.
11.	Koizumi et al., 2020 [12]			an attention process designed to handle time-frequency stretching. displaying significantly better performance compared to conventional methods.	While a promising approach, the proposed SPIDERNET framework lacks flexibility in addressing dynamic domain shifts.
12.	Pustokhina et al., 2021[11]	DADTPW Model	UCSD Anomaly Detection Datase	efficiently recognizes and categorizes abnormalities that appear in the frame according to their superior attributes.	For feature extraction in the two-stage detection approach, a large processing capacity is required.

13.	Aboah et al., 2021.[13]	Multiple models	Real-world dataset (live CCTV)	integrates various techniques, including video [68] sorting and anomaly candidate screening, to improve the model's capacity to identify irregularities in a variety of video sources.	A small change in the data has the potential to induce a substantial change in the decision tree's outcome.
14.	Guansong Pang 2020 [14]	deep neural network	UCSD, Subway, UMN	A method for end-to-end trainable video anomaly detection is presented, which eliminates the requirement for manually labeling normal/abnormal data and allows for combined representation learning and anomaly scoring.	Using the self-training ordinal regression approach, our end-to-end anomaly score learner may improve detection performance iteratively.
15.	Mamoon M. Saeed 2023[16]	Hybrid EL techniques	(CFS-RF). NB2015, CIC_IDS2017, NSL KDD, and CICDDOS2019	A suggested anomaly detection system for 6G networks, called AD6GNs, makes use of ensemble learning (EL) that is tailored for communication networks.	dependable machine learning models are necessary. It is necessary to train models in scenarios that mimic hostile environments in order to create models that are robust against hostile inputs.
16.	Gopikrishna Pavuluri 2023 [17]	neural network with convolutional autoencoder and decoder	UCSD	The encoder network is responsible for extracting spatiotemporal features from video frames and encoding them into a compressed representation. the decoder network generates reconstructed video frames from the encoded representation.	The research focuses on evaluating the effectiveness of larger and more complex video datasets. It explores the utilization of various architectures, including Optical flow and variational autoencoders for anomaly identification in video footage.
17.	Haoyang Jia 2023[18]		MNIST, fMNIST, CIFAR-10	By using two decoders and two encoders in pairs, the method generates two sets of encoder-decoder-encoder (EDE) network architectures. These structures are	The intention is to apply the model to high-resolution photos and extend its applicability to more diverse domains, including medical imaging or security imaging. Additionally, the research aims to explore the model's

				employed to map image distributions to latent distributions that are already defined and vice versa. The technique uses a two-phase training approach designed to mitigate the shortcomings associated with autoencoders (AEs) and generative adversarial networks (GANs). [49]	effectiveness in anomaly detection within video data.
18.	Yu Liu 2020[20]	autoencoder (AE) and the long short-term memory encoder decoder (LSTM-ED)	*CO2 dataset*	The study investigates the viability of using anomaly detection techniques based on machine learning in vertical plant wall systems. The ultimate goal is predictive maintenance for interior climate control with more automation and intelligence.	Using low-cost sensors, working with limited datasets, and improving anomaly detection performance on less often sampled data.
19.	Ahad Alloqmani 2023[19]	deep learning-based anomaly detection [73]	INbreast and MIAS.	The study attempts to identify breast abnormalities, benign and malignant cases included, by considering normal data. To tackle the problem of unbalanced data, the framework includes data pre-processing (image pre-processing, in particular) and feature extraction by using a pre-trained model.	Implement generalization techniques within a framework to enhance adaptability by leveraging local data.
20.	Vafaei Sadr 2023[21]	Deep learning and convolutional neural networks (CNN)	MNIST, CIFAR10, and Galaxy-DECaLS	Improve on established anomaly detection methods to allow the feature space to dynamically evolve, which would enable effective anomaly identification.	Enhance techniques for augmenting anomaly data to provide guidance to the algorithm.

21.	Nedelkoski 2020[22]	anomaly detection approach, Logsy.	Blue Gene/L, hunderbird	Strengthen the security and reliability of computer systems.	The goal of log anomaly detection research is to highlight the diversity of both normal and anomalous data by investigating alternative methods for incorporating richer domain bias. [42]
22.	Muhammad Zaigham Zaheer 2023[75]	one-class classification (OCC),	UCF crime and ShanghaiTech	Using an unsupervised approach to video anomaly detection, generative cooperative learning (GCL) builds a cross-supervision between a discriminator and a generator by taking use of the low frequency of anomalies.	Since anomalies are common in real-world situations, generative cooperative learning, or GCL, is a more realistic approach than oriented comparative analysis (OCC).
23.	Quatrini et al., 2020[1]	Decision Trees	Real-World Dataset	Extensive training times are necessary for model training.	An established anomaly detector method based on decision forests and decision jungles is used, which is especially well-suited for industrial data.
24.	Liu et al., 2020 [2]	Long Short-term memory	Synthetic data and public domain data	When compared to state-of-the-art models, the LSTM and auto-encoder (AE) based models perform better. [59]	Uncommon regularities and outliers or anomalies in the training data might skew the learned feature representations in an autoencoder-based method.
25.	Ganokratanaa et al., 2020 [3]	Convolutional Neural Networks	CUHK Avenue	The proposed approach demands more computation power due to its utilization of Encode and Decode Recurrent Neural Network as its architecture.	The suggested method improves anomaly localization performance at the pixel-level evaluation by applying Edge Wrapping. It also learns typical samples on its own without requiring any parameter changes.
26.	Mehta et al., 2020 [4]			The suggested model can be commercially implemented on any GPU-based system to accurately identify firearms and fire in areas under camera surveillance, resulting in a high detection rate.	The suggested anomaly detection system has the ability to be improved and expanded upon, and it is specifically made for the detection of fires.

27.	Ilyas et al., 2021[5]		PETS 2009	The work proposes the incorporation of a manually crafted feature to capture high-level changes at the frame level, and the combination with a machine learning (ML) and deep learning (DL) model yields improved outcomes.	For the extraction of features at the pixel level, the suggested model is not appropriate.
28.	Liu et al., 2020[6]	Support Vector Machine	Synthetic data and public domain data	The model is trained using a one-class support vector machine (1-SVM) approach, and its performance, along with the algorithms, is assessed using real data sourced from Colorado Water Watch.	The model is trained using a one-class support vector machine (1-SVM) approach, and its performance, along with the algorithms, is assessed using real data sourced from Colorado Water Watch.
29.	Aziz et al., 2021[7]		UMN datasets	The suggested method can lessen erroneous motion anomaly detection and localization alerts because of camera jitter and object motions that happen in unlikely motion zones.	There are temporal and spatial instances when the proposed paradigm is inappropriate. When dealing with datasets that exhibit complex distributions within the normal class, the one-class SVM model is not the best fit.
30.	Alfie et al., 2021[8]	Generative adversarial network	Real-world data (Hajj)	There are temporal and spatial instances when the proposed paradigm is inappropriate. When dealing with datasets that exhibit complex distributions within the normal class, the one-class SVM model is not the best fit.	Further enhancements are required to improve the accuracy of the model, particularly when applied to large-scale crowd datasets.
31.	Barua et al., 2020[9]	Hierarchical Temporal Memory	Benign IoT traffic	The study introduces a real-time anomaly detection approach employing hierarchical temporal memory (HTM) with continual unsupervised learning, requiring	Because the input data for unsupervised learning is unknown and not pre-classified, the results are less reliable.

				no human intervention.	
32.	Zhao et el., 2020[10]	Attention networks	SMAP, MSL TSA,SMAP [39]	The foundation of the research is the dynamic handling of several time series through the use of parallel graph attention layers.	
33.	Koizumi et al., 2020 [12]			In order to manage time-frequency stretching, the study presents an attention technique. The results demonstrate the superiority of this methodology, showing a notable improvement over traditional procedures.	While a promising approach, the proposed SPIDERNET framework lacks flexibility in addressing dynamic domain shifts.
34.	Pustokhina et al., 2021[11]	DADTPW Model	UCSD Anomaly Detection Datase	The suggested method efficiently detects and categorizes abnormalities that arise in the frame according to their superior attributes.	For feature extraction in the two-stage detection approach, a large processing capacity is required.
35.	Aboah et al., 2021.[13]	Multiple models	Real-world dataset (live CCTV)	The research combines multiple methods, such as anomaly candidate filtering and video [68] sorting, to improve the model's ability to identify anomalies in a variety of films.	A small change in the data has the potential to induce a substantial change in the decision tree's outcome.
36.	Guansong Pang 2020 [14]	deep neural network	UCSD, Subway, UMN	A method for end-to-end trainable video anomaly detection is presented, which eliminates the requirement for manually labeling normal/abnormal data and allows for combined representation learning and anomaly scoring.	Using the self-training ordinal regression approach, our end-to-end anomaly score learner may improve detection performance iteratively.

37.	Mamoon M. Saeed 2023[16]	Hybrid EL techniques	(CFS-RF). NB2015, CIC_IDS2017, NSL KDD, and CICDDOS2019	A suggested anomaly detection system for 6G networks, called AD6GNs, makes use of ensemble learning (EL) that is tailored for communication networks.	Machine learning models that are robust are necessary to handle hostile inputs. It is necessary to train models in scenarios that mimic hostile environments in order to create models that are robust against hostile inputs.
38.	Gopikrishna Pavuluri 2023 [17]	convolutional autoencoder and decoder neural network	UCSD	An encoder network and a decoder network are parts of the model architecture. The task of encoding video frames into a compressed representation and extracting spatiotemporal properties from them falls to the encoder network. Concurrently, the encoded representation is used by the decoder network to create reconstructed video frames.	The main goal of the study is to assess how well larger, more intricate video collections perform. It investigates the application of different architectures for anomaly detection in video data, such as variational autoencoders and optical flow.
39.	Haoyang Jia 2023[18]		MNIST, fMNIST, CIFAR-10	The method creates two sets of encoder-decoder-encoder (EDE) network architectures by using two decoders and two encoders in pairs. These structures are used to convert between defined latent distributions and image distributions. In order to address the drawbacks of both generative adversarial networks (GANs) and autoencoders (AEs), the method uses a two-stage training strategy. [49]	The objective is to expand the model's applicability to more varied domains, such as security or medical imaging, and generalize it to high-resolution images. Additionally, the research aims to explore the model's effectiveness in anomaly detection within video data.
40.	Yu Liu 2020[20]	autoencoder (AE) and the long short-term memory encoder	*CO2 dataset*	The study investigates the viability of using anomaly detection techniques based on	improving the performance of cheap sensors, working with limited datasets, and improving anomaly

		decoder (LSTM-ED)		machine learning in vertical plant wall systems. The ultimate goal is predictive maintenance for interior climate control with more automation and intelligence.	detection on less often sampled data.
41.	Ahad Alloqmani 2023[19]	deep learning-based anomaly detection [73]	INbreast and MIAS.	intends to use normal data to identify breast anomalies, including benign and malignant cases. The framework aims to tackle the problem of unbalanced data by implementing data pre-processing techniques, particularly picture pre-processing, and feature extraction by employing a pre-trained model.	Implement generalization techniques within a framework to enhance adaptability by leveraging local data.
42.	Vafaei Sadr 2023[21]	Deep learning and convolutional neural networks (CNN)	MNIST, CIFAR10, and Galaxy-DECaLS	Improve on established anomaly detection methods to allow the feature space to dynamically evolve, which would enable effective anomaly identification.	Enhance techniques for augmenting anomaly data to provide guidance to the algorithm.
43.	Nedelkoski 2020[22]	anomaly detection approach, Logsy.	Blue Gene/L, hunderbird	Strengthen the security and reliability of computer systems.	focus is on exploring alternative approaches to incorporate richer domain bias, emphasizing the diversity of both normal and anomaly data. [42]
44.	Muhammad Zaigham Zaheer 2023[75]	one-class classification (OCC),	UCF crime and ShanghaiTech	Using an unsupervised approach to video anomaly detection, generative cooperative learning (GCL) builds a cross-supervision between a discriminator and a generator by taking use of the low frequency of anomalies.	Since anomalies are common in real-world situations, generative cooperative learning, or GCL, is a more realistic approach than oriented comparative analysis (OCC).

The literature review encompasses various studies on anomaly detection using machine learning. In the study by [51] Quatrini et al. (2020) [1], Decision Trees were employed in a decision forest and decision jungle-based approach for anomaly detection and process phase classification. The research emphasized the practical application of the proposed method in industrial settings, using a real-world dataset. However, it noted the drawback of extensive training times required for model training. Liu et al. (2020) [2] investigated anomaly detection [57] in IoT-based vertical plant walls for indoor climate control, employing Long Short-term Memory (LSTM) and autoencoder (AE) based models. The study revealed superior performance but highlighted the challenge of distorted feature representations in the presence of uncommon regularities or outliers in the training data. [48] Ganokratanaa et al. (2020) [3] proposed an unsupervised anomaly detection and localization approach using a deep spatiotemporal translation network. The study, utilizing Convolutional Neural Networks (CNNs) and the CUHK Avenue dataset, demonstrated enhanced [74] anomaly localization at the pixel level. However, it noted the increased computation power demand due to the architecture involving Encode and Decode Recurrent Neural Networks.[65] Mehta et al. (2020) [4] presented an anomaly detection system for fire and gun violence using deep neural networks, deployable on GPU-based systems. The study emphasized its suitability for commercial use but acknowledged the need for potential improvement and diversification, especially considering its specificity to fire detection. [50] Ilyas et al. (2021) [5] introduced a hybrid deep network-based approach for crowd anomaly detection, combining manually crafted features with machine learning (ML) and deep learning (DL) models. While achieving improved outcomes, the study noted the model's limitation in pixel-level feature extraction. Liu et al. (2020) [6] focused on machine learning and transport simulations for groundwater anomaly detection, [45] utilizing a one-class support vector machine (1-SVM) approach. The study evaluated the model on real data from Colorado Water Watch, emphasizing its performance assessment with both synthetic and public domain data. Aziz et al. (2021) [7] investigated video anomaly detection and localization based on appearance and motion models, aiming to reduce false alarms in complex scenarios. The study, using UMN datasets, highlighted the model's unsuitability for spatial and temporal scenarios and its limitations with complex distributions in the normal class. Alfie et al. (2021) [8] explored generative adversarial network-based abnormal behavior detection in massive crowd videos, specifically focusing on a Hajj case study. The study emphasized the model's limitations in spatial and temporal scenarios and the need for further enhancements, particularly for large-scale crowd datasets. Barua et al. (2020) [9] proposed a real-time anomaly detection approach using hierarchical temporal memory (HTM) in smart grids. The study focused on benign IoT traffic, noting the challenges of less accurate outputs in unsupervised learning. Zhao et al. (2020) [10] investigated multivariate time-series anomaly detection via a graph attention network, addressing various time series. While utilizing datasets from NASA, the study highlighted a significant limitation in the model's inability to learn topological structures among sensors. Koizumi et al. (2020) [12] introduced SPIDERnet for one-shot anomaly detection in sounds, demonstrating superior performance but noting the framework's lack of flexibility in addressing dynamic domain shifts. Pustokhina et al. (2021) [11] presented an automated deep learning-based anomaly detection system for pedestrian walkways, emphasizing effectiveness and the computational requirements for feature extraction. Aboah et al. (2021) [13] proposed a vision-based system for traffic anomaly detection, incorporating video sorting and anomaly candidate filtering. The study noted the sensitivity of decision trees to small changes in data. Guansong Pang (2020) [14] introduced a self-trained deep ordinal regression approach for end-to-end video anomaly detection, leveraging datasets from UCSD, Subway, and UMN. The study highlighted the model's capability for iterative enhancement of detection performance. Mamoon M. Saeed (2023) [16] proposed an anomaly detection system for 6G networks using ensemble learning (EL) techniques, emphasizing the need for robust models to handle adversarial inputs. Gopikrishna Pavuluri (2023) [17] presented a deep learning approach to video anomaly detection using convolutional autoencoders, exploring various architectures and datasets from UCSD. Haoyang Jia (2023) [18] investigated anomaly detection in images using shared autoencoders, focusing on generalization to high-resolution images [53] and diverse domains. Yu Liu (2020) [20] explored anomaly detection in IoT-based vertical plant walls, emphasizing the feasibility of machine learning methods for predictive maintenance. Ahad Alloqmani (2023) [19] aimed to detect breast cancer anomalies using deep learning, addressing imbalanced data and recommending generalization techniques. Vafaei Sadr (2023) [21] proposed personalized anomaly detection using deep active learning, emphasizing dynamic evolution of the feature space and the need for data augmentation techniques

[36]. Nedelkoski (2020) [22] strengthened computer system security with a self-attentive classification-based anomaly detection approach, focusing on richer domain bias in log data. Muhammad Zaigham Zaheer's work in "Generative Cooperative Learning for Unsupervised Video Anomaly Detection" (2023) introduces a novel approach, the Generative Cooperative Learning (GCL), designed for unsupervised video anomaly detection. This method strategically leverages the infrequent occurrence of anomalies by establishing cross-supervision between a generator and a discriminator. The study compares GCL with traditional one-class classification (OCC) methods and emphasizes the increased realism of GCL in real-world scenarios where anomalies are natural events. The research is validated through extensive experiments on UCF crime and ShanghaiTech datasets, demonstrating GCL's effectiveness and positioning it as a promising alternative for unsupervised video anomaly detection [75].

3. Materials and Methods

3.1. Complexities for identifying the anomaly

Anomaly detection is a crucial aspect of data analysis and machine learning, and it involves identifying patterns or data points that deviate significantly from the expected or normal behavior within a dataset. [27],[28]The characteristics of anomaly detection methods can vary based on the approach used, but some common features and considerations include [71]

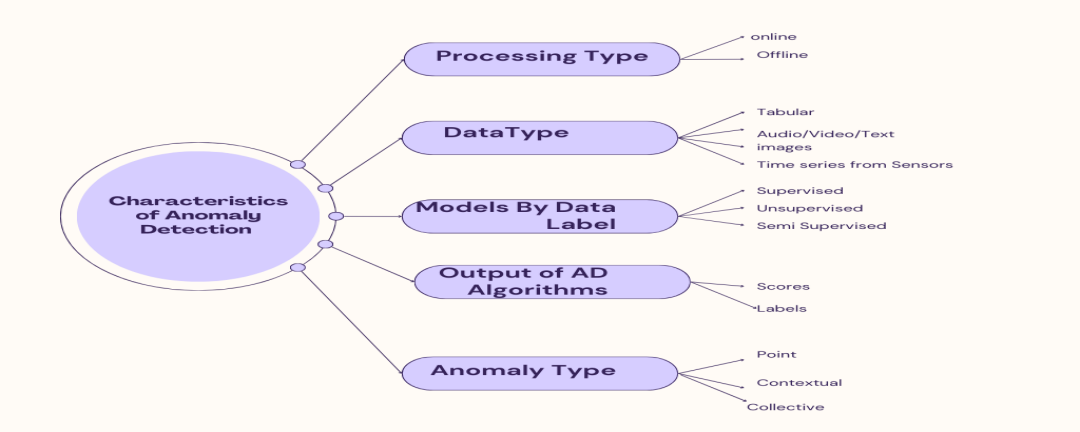

Figure 1. Characteristics of Anomaly detection

3.1.1. Supervised Learning

Supervised learning involves training an algorithm on a labeled dataset, where input data is associated with corresponding output labels. The objective is for the algorithm to grasp the mapping or correlation between input features and their respective output labels. Following training, the model can then make predictions or classifications on novel, unseen data. Applications of supervised learning encompass tasks such as image recognition, speech recognition, and solving classification problems. As mentioned in Figure 1.

3.1.2. Unsupervised Learning

Many [64] anomaly detection methods are based on unsupervised learning, where the model is trained on a dataset without explicit labels for normal and anomalous instances. This flexibility is advantageous when labeled anomaly data is scarce or unavailable. Unsupervised learning involves training the algorithm on an unlabeled dataset, where the input data is not paired with corresponding output labels. The goal is typically to find patterns, structures, or relationships within the data. Unsupervised learning encompasses tasks such as clustering, wherein the algorithm aggregates akin data points, and dimensionality reduction, where the algorithm streamlines the dataset while preserving crucial information. An example of unsupervised learning is clustering similar customer behaviors based on purchase history.

3.1.3. Semi-Supervised Learning

Semi-supervised learning is a composite methodology that amalgamates facets of both supervised and unsupervised learning. In this scenario, the dataset is partially labeled, meaning that some data points have associated output labels, while others do not. The algorithm utilizes the annotated data to discern

patterns and correlations, subsequently extrapolating this acquired knowledge to render predictions or classifications on the unannotated data. Semi-supervised learning is particularly useful when obtaining a fully labeled dataset is expensive or time-consuming. An example is using a partially labeled dataset for training a model to classify emails as spam or not spam.

3.1.4. Normal Behavior Modeling:

Anomaly detection methods typically involve the construction of a model representing normal behavior or patterns within the data. This model serves as a reference point for identifying deviations. Anomaly detection algorithms, particularly those based on supervised or unsupervised learning, begin by training on a dataset that is presumed to contain only normal instances. This dataset is often referred to as the "training set."

- Feature Extraction and Representation:
- Model Construction
- Threshold Setting
- Dynamic Adaptation
- Evaluation and Tuning

3.2. Data Characteristics

Anomaly detection algorithms often assume that normal instances follow a certain distribution, and deviations from this distribution are considered anomalies. The distribution may be Gaussian, uniform, or exhibit other specific characteristics. Anomalies are typically rare events compared to normal instances, leading to imbalanced datasets. Anomaly detection methods need to address imbalanced data to prevent models from being biased toward the majority class. In scenarios involving time series data, the temporal aspects are critical. Anomalies may manifest as sudden spikes, drops, or unusual patterns over time. Time-dependent characteristics must be considered in the modeling process. Seasonal patterns or recurring trends in time series data can impact anomaly detection. Understanding and accounting for seasonality are essential to distinguish between expected variations and anomalous behavior. The number of features or dimensions in the dataset influences the choice of anomaly detection methods. Noisy data, containing errors or outliers unrelated to anomalies, can pose challenges for anomaly detection. Preprocessing steps may be required to clean the data and improve the accuracy of anomaly detection models. Domain-specific knowledge about the data and potential anomalies is valuable. Incorporating domain expertise can help in feature selection, model interpretation, and setting appropriate thresholds for anomaly detection. In some applications, the characteristics of normal behavior may change over time. Anomaly detection models should be capable of adapting to these dynamic changes to maintain effectiveness.

3.2.1. Scalabilityand real time processing

Anomaly detection methods should be scalable to handle large datasets efficiently. This scalability is crucial for applications in industries such as finance, cybersecurity, and industrial operations, where datasets can be extensive. Depending on the application, anomaly detection may need to operate in real-time or in batch processing mode [67]. Real-time processing is critical for scenarios where swift identification and response to anomalies are required.

3.3. Techniques and Models of Machine Learning (ML) and Deep Learning (DL)

In traditional machine learning, [56] there is a reliance on manual feature engineering, whereas deep learning excels in the automatic acquisition of hierarchical representations. Deep learning models demand substantial computational resources and frequently necessitate robust hardware, particularly GPUs, in contrast to numerous conventional machine learning models. Machine learning models are often more interpretable, making them suitable for applications where transparency is crucial. Deep learning models are sometimes considered black boxes. Each deep learning and machine learning exhibit unique strengths and limitations, with the decision between them contingent on the particular problem at hand, the existing dataset, and the computational resources accessible. Both deep learning and machine learning reside within the realm of artificial intelligence (AI), concentrating on the formulation of algorithms and models endowed with the capacity to learn and render predictions or decisions. Machine learning [54] encompasses a broader scope, entailing the creation of algorithms and models that empower computers to glean insights from data, progressively refining their performance on a designated task without the need for explicit programming. [38]

3.4. ML and DL Algorithms for Anomaly Detection

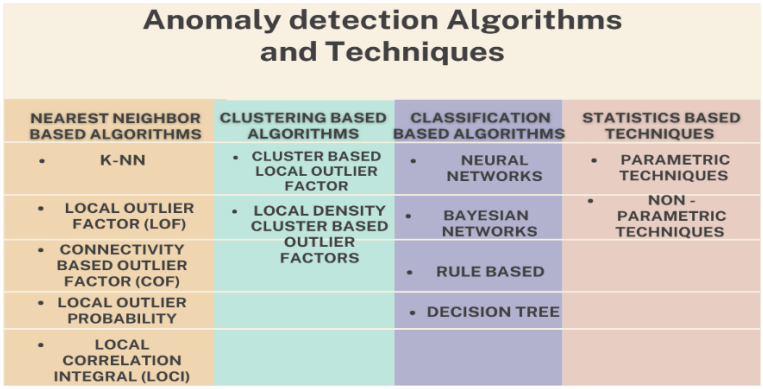

Figure 2. Anomaly Detection Algorithms and Techniques

There are various algorithms and techniques used in anomaly detection, each suited to different types of data and specific use cases. [43] Here are some common algorithms used in anomaly detection:

3.4.1. Nearest neighbor based algorithms

Nearest neighbor-based algorithms are a family of methods for anomaly detection that rely on measuring the proximity of data points to their neighbors. These algorithms identify anomalies based on the premise that anomalies are points that deviate significantly from their neighbors in the feature space. Here are some common nearest neighbor-based algorithms used in anomaly detection: k-Nearest Neighbors (k-NN): An instance is classified as an anomaly if it has fewer than k neighbors within a specified distance [61]. Calculate the distances from the data point to its k-nearest neighbors. If the point is an outlier, it will have fewer nearby neighbors. k-NN is adaptable and can be employed across diverse data types, rendering it well-suited for both global and local anomaly detection. Local Outlier Factor (LOF): Quantifies the deviation in local density for a given data point in comparison to its neighbors. LOF computes the ratio between the local density of a point and the local density of its neighboring points. Anomalies have lower density compared to their neighbors. Effective for detecting anomalies in datasets with varying densities, making it suitable for applications where anomalies may appear in clusters. Isolation Forest: Focuses on isolating anomalies by creating partitions in the feature space. Creates a collection of isolation trees, wherein each tree is a binary structure constructed by randomly choosing features and splitting values. Anomalies are expected to be isolated with fewer splits. Particularly useful when anomalies are rare and can be isolated more quickly than normal instances. Angle-Based Outlier Detection (ABOD): Measures the variability in angles between data points in the feature space. [44] Calculates the variance of angles formed between a specific data point and all other points in the dataset. Anomalies are expected to have higher angle variances. Suitable for datasets where anomalies exhibit different directionalities than normal instances. HBOS (Histogram-Based Outlier Score): Constructs histograms to estimate the distribution of normal data. Calculates an outlier score based on the density of the bin where a data point falls. Unusual bins indicate potential anomalies. Efficient for high-dimensional data and datasets with a skewed distribution. Nearest neighbor-based algorithms are intuitive and computationally efficient, making them applicable to a wide range of domains. However, their performance can be sensitive to the choice of distance metric, the definition of neighbors, and the value of parameters such as k. Experimentation and fine-tuning are often required to achieve optimal results for a specific dataset and application.

3.4.2. Clustering based algorithms

Clustering-based algorithms for anomaly detection aim to [46] group similar data points together and identify anomalies as instances that do not conform to any cluster [34]. These algorithms leverage the concept that anomalies often exhibit characteristics that distinguish them from the majority of the data, making them less likely to belong to any specific cluster. Here are some common clustering-based algorithms used in anomaly detection: k-Means, partitioning the dataset into k clusters according to their similarity, anomalies are defined as instances that do not align well with any specific cluster. The distance between a point and its cluster center can serve as a metric for anomaly assessment [35]. Anomalies are

points with low density-reachability, indicating that they are not part of a well-defined cluster. Effective for datasets with varying cluster densities and complex structures. Mean Shift: Locates modes or peaks of data density. Anomalies are points that do not converge to any mode, indicating they are distant from high-density regions. Suitable for datasets with irregularly shaped clusters and varying densities. Hierarchical Clustering, builds a tree-like hierarchy of clusters. Anomalies can be identified as points that do not neatly fit into any hierarchical level or exhibit inconsistencies in clustering. Useful when the dataset has a nested or hierarchical structure. Gaussian Mixture Models (GMM), operates under the assumption that the data is produced by a combination of Gaussian distributions [40]. Anomalies are instances with low likelihoods under the Gaussian mixture model. Effective for datasets with multiple overlapping clusters. Self-Organizing Maps (SOM), utilizes a neural network approach to map high-dimensional data onto a lower-dimensional grid. Anomalies are discerned as data points positioned significantly distant from the customary clusters on the SOM grid. Suitable for visualizing and clustering high-dimensional data. When using clustering-based algorithms for anomaly detection, it's important to consider factors such as the number of clusters, the choice of distance metric, and the interpretation of cluster assignments. Additionally, these algorithms may not perform well when anomalies form their own clusters or when the normal data exhibits complex structures. Experimentation and parameter tuning are crucial to achieving effective anomaly detection using clustering-based approaches.

3.4.3. Classification based algorithms

Classification-based algorithms for anomaly detection involve training a model to distinguish between normal and anomalous instances based on labeled training data. These algorithms learn a decision boundary or a classification rule that separates normal behavior from anomalies. Support Vector Machines (SVM) constructs a hyperplane that maximally separates normal instances from anomalies in a high-dimensional space. Anomalies are instances lying on the wrong side of the hyperplane or with a large margin from the decision boundary. Effective for both linear and non-linear separation of normal and anomalous instances [31], [32]. Random Forest, ensemble learning method that constructs multiple decision trees. Anomalies can be identified by measuring the lack of support from individual decision trees or by considering the distribution of anomaly scores across the ensemble. Versatile and applicable to various types of data, suitable for datasets with complex structures. Decision Trees, constructs a tree-like structure of decisions based on features. Anomalies are identified by the path they take through the decision tree or by considering leaf nodes associated with fewer instances [32]. Applications: Simple and interpretable, suitable for datasets with clear decision boundaries. Logistic Regression, models the relationship between input features and the likelihood of an instance being anomalous. Anomalies are identified based on the predicted probabilities or the decision boundary learned by the logistic regression model. Suitable for binary classification tasks with a linear decision boundary. Naive Bayes, assumes independence between features and calculates the probability of an instance being anomalous. Anomalies are identified based on the calculated probabilities, and the decision is made using a predefined threshold. Simple and computationally efficient, suitable for datasets with categorical features. Neural Networks, deep learning models with multiple layers that learn complex representations of data. Anomalies can be identified based on the output layer's activation patterns or by measuring reconstruction errors in auto encoder architectures [29], [30]. Effective for high-dimensional data and complex patterns, suitable for a wide range of applications. Ensemble of Classifiers, combines predictions from multiple classifiers. Anomalies can be identified based on the disagreement among ensemble members or by aggregating individual anomaly scores. Enhances robustness and generalization, useful when individual classifiers may be sensitive to certain types of anomalies. Gradient Boosting, Builds a series of weak learners to create a strong predictive model. Anomalies can be identified based on the boosting process, where subsequent weak learners focus on instances that are difficult to classify. Useful for improving model accuracy over time, particularly in datasets with imbalanced classes. When using classification-based algorithms for anomaly detection, it's crucial to have a well-labeled dataset that includes both normal and anomalous instances for training. The choice of algorithm depends on the characteristics of the data, the nature of anomalies, and the interpretability requirements of the application. Fine-tuning and experimentation are often necessary to achieve optimal performance.

3.4.4. Statics based techniques

Statistical-based techniques for anomaly detection rely on the assumption that normal behavior follows a specific statistical distribution, and anomalies deviate significantly from this expected distribution. These methods use statistical measures to identify instances that are unlikely to occur under normal circumstances. Anomalies are identified as instances with high or low z-scores, indicating they deviate significantly from the mean. Simple and effective for univariate data, where anomalies exhibit extreme values. Modified Z-Score, a robust version of the standard z-score, resistant to the influence of outliers. Anomalies are identified based on modified z-scores, which consider the median and median absolute deviation instead of the mean and standard deviation. Suitable for datasets with outliers that may affect the accuracy of the standard z-score. Grubbs' Test (Maximum Deviation from Mean), etects a single outlier in a univariate dataset. Anomalies are identified based on the maximum absolute deviation from the mean. Effective for identifying isolated anomalies in univariate data. Hampel Identifier, a robust method for detecting outliers in time series data. Uses Hampel identifier to identify anomalies based on median absolute deviation. Suitable for time series data with variations in both amplitude and frequency. Q-Q Plots (Quantile-Quantile Plots), graphical method to assess if a dataset follows a particular theoretical distribution. Anomalies are detected by visually inspecting deviations from the expected quantiles. Useful for assessing whether data follows a known distribution an identifying anomaly. Kolmogorov-Smirnov Test, non-parametric test to assess whether a sample follows a specific distribution. Compares the cumulative distribution function of the sample to the expected distribution. Effective for identifying differences between the empirical and expected distributions. Chauvenet's Criterion, a method for identifying outliers in a normally distributed dataset. Uses Chauvenet's criterion to calculate a critical threshold for identifying anomalies. Suitable for univariate data with a normal distribution. Histogram-Based Outlier Score (HBOS), a onstructs histograms to estimate the distribution of normal data. [55] Anomalies are identified based on the density of the bin where a data point falls. Efficient for high-dimensional data and datasets with a skewed distribution. These statistical-based techniques are often used for univariate data or when certain assumptions about the distribution of data can be reasonably made. They are generally simpler to implement and interpret, making them suitable for scenarios where the statistical properties of normal behavior are well understood. However, their effectiveness may be limited in complex, high-dimensional datasets or when the assumptions about the data distribution are not met.

3.5 Challenges faced: Working on Anomaly Data

Deep learning excels in discerning intricate patterns within vast datasets. Anomaly detection leverages this capability to identify deviations from normal patterns, even in highly complex and multidimensional data. Anomaly detection using machine learning and deep learning approaches comes with its own set of challenges. Some of the common challenges include:

3.5.1. Adaptability to Diverse Data Types and dataset

Anomaly detection using deep learning is not constrained by the type of data. Whether it's images, time series, textual data, or a combination of these, deep learning models can adapt and learn nuanced representations, making them versatile for anomaly detection across various domains. [23]

3.5.2. Automated Learning and Imbalanced Datasets

Anomalies are often rare events compared to normal instances, leading to imbalanced datasets. [23] Class imbalance can affect the performance of models, making them biased toward the majority class. Special techniques, such as oversampling anomalies or adjusting class weights, may be required. The selection and quality of the dataset are pivotal factors influencing the effectiveness of anomaly detection models. Several issues related to datasets can impact the performance and reliability of anomaly detection methods. Anomalies typically represent infrequent occurrences compared to normal instances, creating imbalances in datasets. Such imbalances can lead to model bias toward the majority class, posing challenges for effective anomaly detection. Obtaining labeled data for anomalies can be difficult and expensive. Anomalies, by their nature, are often rare, making it impractical to have a well-labeled dataset for training. Noisy data, outliers, or errors in the dataset that are not indicative of true anomalies can impact the performance of anomaly detection models. In dynamic environments where normal behavior changes over time, static datasets may become outdated, leading to reduced model effectiveness. The dataset may not fully represent all possible variations and scenarios in the real-world environment, leading to models that may not generalize well. Anomalies in time series data may not always be well-represented

in the dataset, and the temporal characteristics of anomalies may not align with the training data. Selecting relevant features that effectively capture normal and anomalous behavior is a critical aspect of anomaly detection [23].

3.5.3. Scalability and Big Data Handling

In an era of big data, deep learning models exhibit scalability, enabling effective analysis of massive datasets. Anomaly detection benefits from this scalability, providing a robust solution for identifying rare events within extensive and diverse data sources. Anomaly detection may need to scale to handle large datasets in real-time or near real-time scenarios [72]. Efficient algorithms and scalable architectures are crucial to process and analyze extensive data volumes effectively.

3.5.4. High-Dimensional Data with time Detection and Rapid Response

Many real-world datasets are high-dimensional, meaning they contain a large number of features [63]. Traditional machine learning algorithms may struggle with the curse of dimensionality. Techniques like feature selection or dimensionality reduction are often required. Deep learning models, when optimized, can operate in real-time, enabling the immediate detection of anomalies. This capability is crucial in scenarios such as cybersecurity, where swift identification of irregularities is paramount for preventing security breaches and mitigating risks.

3.5.5. Complexity of Models and Enhanced Accuracy

Deep learning models, while powerful, can be complex and computationally expensive. Training deep neural networks may require substantial computational resources, and the interpretability of these models can be challenging. The inherent depth and complexity of deep learning architectures contribute to higher accuracy in distinguishing anomalies from normal patterns. This reduces false positives, ensuring that identified anomalies are more likely to be genuine threats or deviations.

3.5.6. Labeling and extraction of Anomalies

Obtaining labeled data for anomalies can be difficult and expensive. In many cases, anomalies are rare, making it impractical to have a well-labeled dataset for training. Unsupervised and semi-supervised methods are often used to address this challenge. Deep learning models autonomously learn relevant features from data, eliminating the need for manual feature engineering. This automated learning is particularly advantageous for anomaly detection, where anomalies may manifest in unexpected ways. Continuous Learning and Adaptation of Dynamic Environments, anomaly detection models may struggle to adapt to dynamic environments where normal behavior changes over time. The ability to detect anomalies in evolving systems requires continuous monitoring and retraining of models. Deep learning models can continuously learn and adapt to evolving patterns in data. This adaptability is crucial for anomaly detection systems to remain effective over time, as the nature of anomalies may change or become more sophisticated.

3.5.7. Noise, Interpretability and Outliers

Noise or outliers in the data, which are not true anomalies, can impact the performance of anomaly detection models. Preprocessing steps are often required to clean the data and mitigate the impact of irrelevant outliers [31]. Deep learning models, particularly neural networks, are frequently characterized as "black boxes," introducing difficulty in interpreting the rationale behind specific decisions [52]. Interpretability is crucial in applications where understanding the reasons for anomaly detection is important. Transferability and Unsupervised Learning for Unknown Anomalies: Anomaly detection models trained on one type of data may not generalize well to other types of data. Transfer learning approaches may be needed to adapt models to different domains or applications. Deep learning models, particularly in unsupervised settings, can discover anomalies without prior knowledge of specific patterns.

3.5.8. Adversarial Attack, Data Privacy and Security

Deep learning models, in particular, are vulnerable to adversarial attacks, where malicious actors seek to manipulate input data to deceive the model [47]. Developing robustness against such attacks remains an ongoing challenge in research [70]. Anomaly detection often involves sensitive data, particularly in areas like healthcare or finance. Ensuring the privacy and security of the data, as well as complying with regulations, can be a significant challenge.

3.5.9. Threshold Selection

Setting an appropriate threshold for defining anomalies is a non-trivial task. It often requires a balance between minimizing false positives and false negatives, [62] and the optimal threshold may vary

depending on the specific application. The application of anomaly detection in conjunction with deep learning spans various industries, including finance, healthcare, manufacturing, and more. It plays a pivotal role in safeguarding financial transactions, identifying unusual health conditions, and ensuring the quality of manufacturing processes. These challenges require a combination of algorithmic advancements, careful data preprocessing, and domain-specific considerations. Researchers and practitioners continue to explore novel techniques to improve the robustness and effectiveness of anomaly detection methods [60]. In summary, the marriage of anomaly detection and deep learning represents a paradigm shift in our ability to identify irregularities within complex datasets. This symbiotic relationship has far-reaching implications, enhancing our capacity to secure systems, optimize processes, and extract meaningful insights from the ever-expanding realm of data.

4. Results

In this review article on anomaly detection using deep learning techniques, the contribution lies in addressing and elucidating the challenges and issues faced by researchers in the initial stages of their work in this domain [66]. The primary motivation is to shed light on the complexities encountered when embarking on anomaly detection projects. Identification of Anomalies is the biggest challenge to be faced. The initial challenge involves accurately identifying anomalies and understanding their diverse types and characteristics. The contribution in this article delves into the intricacies of anomaly identification, providing insights into various types and characteristics, thereby offering a foundational understanding for researchers entering this field. Then the second biggest issue is in selection of Deep Learning Models where Researchers face the task of selecting the most suitable deep learning model from the plethora of available options for anomaly detection. The contribution in this review comprehensively explores different deep learning models, offering a nuanced understanding of their strengths and weaknesses. This facilitates the decision-making process for researchers, making it easier to select an appropriate model for their specific anomaly detection needs. Then the last and most important task is to take Comparative Analysis of Research Outputs. With a multitude of research outputs on anomaly detection using deep learning, it can be challenging to discern the most effective models and approaches. The article systematically reviews and compares the work done by various researchers, providing a valuable synthesis of their learnings and outputs. This comparative analysis aids in identifying trends, successful methodologies, and ultimately suggests the most accurate models for effective anomaly detection. Another challenge that has been discussed in this research work is Integration of Machine Learning Algorithms. In the broader context of the study, the challenge extends to determining the best approach for outlier detection by considering various machine learning algorithms. The article presents, implements, applies, and evaluates different machine learning algorithms, contributing to the decision-making process regarding the optimal approach for outlier detection analysis.

5. Discussion

This research comprehensively assesses the performance of deep learning-based anomaly detection methods in video sequences, specifically focusing on publicly available datasets. The presented table categorizes various approaches based on the type of learning applied and the datasets utilized. The analysis underscores a notable preference for unsupervised learning methods, chosen for their efficacy in learning representations without the need for labeled video data. While unsupervised methods effectively handle the complexity and diverse visual behaviors of anomalies in unconstrained environments, their overall performance remains limited. To address this, some researchers opt for semi-supervised learning methods, leveraging data related only to the "normal" class, offering greater specificity in anomaly detection compared to purely unsupervised methods. Despite considerable research, challenges persist, especially in adapting anomaly detection algorithms designed for regular scenes to less structured situations.

Real-time application in unconstrained environments and addressing time complexity emerge as critical considerations. In this context, the Generative Cooperative Learning (GCL) approach stands out as a superior method for unsupervised video anomaly detection compared to traditional one-class classification (OCC) approaches. GCL's strength lies in strategically leveraging the infrequent occurrence of anomalies through cross-supervision between a generator and a discriminator. This enables GCL to capture the unique characteristics of anomalies, enhancing adaptability to real-world scenarios where anomalies are natural events. Demonstrating increased realism, GCL proves well-suited for complex and dynamic environments. The research validates GCL's effectiveness through extensive experiments on UCF crime and ShanghaiTech datasets, positioning it as a promising alternative in unsupervised video anomaly detection

6. Conclusions

This research endeavors to underscore the formidable challenges and intricacies encountered by researchers immersed in the domain of anomaly detection through the application of deep learning methodologies. The underlying impetus for this investigation lies in the elucidation of the preliminary hurdles and complexities confronted during the initiation of anomaly detection projects. The foremost challenge resides in the precise identification and categorization of anomalies, wherein this paper provides a comprehensive delineation of diverse anomaly types and their inherent characteristics. Moreover, the research grapples with the multifaceted challenge of discerning and selecting the most optimal deep learning model from a myriad of available alternatives for effective anomaly detection. To streamline this process, the study expounds upon various deep learning models, offering a nuanced exposition of their respective attributes. Furthermore, the research conducts a meticulous review of diverse studies undertaken by researchers in the realm of anomaly detection. This includes a detailed examination of their methodologies, findings, and outputs, culminating in a comparative analysis. The objective is to distill key insights from this collective body of work, facilitating the identification of the most accurate and efficacious deep learning model. Within the purview of this investigation, a diverse array of machine learning algorithms is presented, implemented, and applied. These algorithms are systematically evaluated to determine the optimal approach for outlier detection analysis. This comprehensive approach contributes to the discourse by not only addressing the challenges inherent in anomaly detection using deep learning but also by presenting a synthesized understanding of the most effective methodologies and models in the field. This study integrates the most recent and thorough examination of cutting-edge research conducted between 2020 and 2023.

This research work contains numerous datasets employed in experiments featured in relevant research publications. A majority of these experiments utilize real-world datasets for training or testing their models. Our analysis unveils that several avenues are still in their early stages and demand substantial research. Additionally, many datasets are becoming outdated, being supplanted by newer and more pertinent real-world datasets, enhancing their value. This review serves as a valuable starting point for researchers and the AI community, offering up-to-date and pertinent insights into anomaly detection using machine learning techniques [54].

References

1. Quatrini, Elena, Francesco Costantino, Giulio Di Gravio, and Riccardo Patriarca. "Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities." Journal of Manufacturing Systems 56 (2020): 117-132
2. Liu, Yu, Zhibo Pang, Magnus Karlsson, and Shaofang Gong. "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control." Building and Environment 183 (2020): 107212.
3. Ganokratanaa, Thittaporn, Supavadee Aramvith, and Nicu Sebe. "Unsupervised anomaly detection and localization based on deep spatiotemporal translation network." IEEE Access 8 (2020): 50312-50329
4. Mehta, Parth, Atulya Kumar, and Shivani Bhattacharjee. "Fire and gun violence based anomaly detection system using deep neural networks." In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 199-204. IEEE, 2020
5. Ilyas, Zirgham, Zafar Aziz, Tehreem Qasim, Naeem Bhatti, and Muhammad Faisal Hayat. "A hybrid deep network based approach for crowd anomaly detection." Multimedia Tools and Applications 80, no. 16 (2021): 24053-24067.
6. Liu, Jiangguo, Jianli Gu, Huishu Li, and Kenneth H. Carlson. "Machine learning and transport simulations for groundwater anomaly detection." Journal of Computational and Applied Mathematics 380 (2020): 112982.
7. Aziz, Zafar, Naeem Bhatti, Hasan Mahmood, and Muhammad Zia. "Video anomaly detection and localization based on appearance and motion models." Multimedia Tools and Applications 80, no. 17 (2021): 25875-25895
8. Alafif, Tarik, Bander Alzahrani, Yong Cao, Reem Alotaibi, Ahmed Barnawi, and Min Chen. "Generative adversarial network based abnormal behavior detection in massive crowd videos: a hajj case study." Journal of Ambient Intelligence
9. Barua, Anomadarshi, Deepan Muthirayan, Pramod P. Khargonekar, and Mohammad Abdullah Al Faruque. "Hierarchical temporal memory based machine learning for real-time, unsupervised anomaly detection in smart grid: WiP abstract." In 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), pp. 188-189. IEEE, 2020.
10. Zhao, Hang, Yujing Wang, Juanyong Duan, Congrui Huang, Defu Cao, Yunhai Tong, Bixiong Xu, Jing Bai, Jie Tong, and Qi Zhang. "Multivariate time-series anomaly detection via graph attention network." In 2020 IEEE International Conference on Data Mining (ICDM), pp. 841-850. IEEE, 2020.
11. Pustokhina, Irina V., Denis A. Pustokhin, Thavavel Vaiyapuri, Deepak Gupta, Sachin Kumar, and K. Shankar. "An automated deep learning based anomaly detection in pedestrian walkways for vulnerable road users safety." Safety science 142 (2021): 105356.
12. Koizumi, Yuma, Masahiro Yasuda, Shin Murata, Shoichiro Saito, Hisashi Uematsu, and Noboru Harada. "Spidernet: Attention network for one-shot anomaly detection in sounds." In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 281-285. IEEE, 2020.
13. Aboah, Armstrong. "A vision-based system for traffic anomaly detection using deep learning and decision trees." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4207-4212. 2021.
14. G. Pang, C. Yan, C. Shen, A. van den Hengel, and X. Bai, "Self-Trained Deep Ordinal Regression for End-to-End Video Anomaly Detection," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, Jun. 2020, pp. 12170–12179, doi: 10.1109/CVPR42600.2020.01219.
15. A. Atghaei, S. Ziaeinejad, and M. Rahmati, "Abnormal Event Detection in Urban Surveillance Videos Using GAN and Transfer Learning," arXiv:2011.09619 [cs], Nov. 2020, Accessed: May 17, 2021. [Online]. Available: http://arxiv.org/abs/2011.09619
16. Mamoon M. Saeed, Rashid A. Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly Detection in 6G Networks Using Machine Learning Methods. Electronics, 12(15), 3300. https://doi.org/10.3390/electronics12153300
17. Pavuluri, G., & Annem, G. (Year). A Deep Learning Approach to Video Anomaly Detection using Convolutional Autoencoders. arXiv preprint arXiv:2311.04351.
18. Jia, H., & Liu, W. (2023). Anomaly detection in images with shared autoencoders. Frontiers in Robotics and AI, 10, Article 1046867. https://doi.org/10.3389/fnbot.2022.1046867
19. Alloqmani, A., Abushark, Y. B., & Khan, A. I. (2023). Anomaly Detection of Breast Cancer Using Deep Learning. Arabian Journal for Science and Engineering, 48(12), 10977–11002. https://doi.org/10.1007/s13369-023-07945-z
20. Liu, Y., Pang, Z., Karlsson, M., & Gong, S. (2020). Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control. Building and Environment, 183, 107212. https://doi.org/10.1016/j.buildenv.2020.107212
21. Vafaei Sadr, A., Bassett, B. A., & Sekyi, E. (2023). Personalized anomaly detection using deep active learning. RASTAI, 2, 586–598. https://doi.org/10.1093/rasti/rzad032
22. Nedelkoski, S., Bogatinovski, J., Acker, A., Cardoso, J., & Kao, O. (2020). Self-Attentive Classification-Based Anomaly Detection in Unstructured Logs. arXiv preprint arXiv:2008.09340.
23. Jiang, Xinwei, Junbin Gao, Xia Hong, and Zhihua Cai. "Gaussian processes autoencoder for dimensionality reduction." In Pacific-Asia conference on knowledge discovery and data mining, pp. 62-73. Springer, Cham, 2014.
24. Grubbs, Frank E. "Procedures for detecting outlying observations in samples." Technimetrics 11, no. 1 (1969): 1-21.
25. Agrawal, Shikha, and Jitendra Agrawal. "Survey on anomaly detection using data mining techniques." Procedia Computer Science 60 (2015): 708-713.
26. Gogoi, Prasanta, Dhruba K. Bhattacharyya, Bhogeswar Borah, and Jugal K. Kalita. "A survey of outlier detection methods in network anomaly identification." The Computer Journal 54, no. 4 (2011): 570-588.

27. Chandola, Varun, Arindam Banerjee, and Vipin Kumar. ”Anomaly detection: A survey.” ACM computing surveys (CSUR) 41, no. 3 (2009): 1-58.
28. Chandola, Varun, Arindam Banerjee, and Vipin Kumar.”Anomaly detection for discrete sequences: A survey.” IEEE transactions on knowledge and data engineering 24, no. 5 (2010): 823-839.
29. Williams, Graham, Rohan Baxter, Hongxing He, Simon Hawkins, and Lifang Gu. ” A comparative study of RNN for outlier detection in data mining.” In 2002 IEEE International Conference on Data Mining, 2002. Proceedings., pp. 709-712. IEEE, 2002.
30. Hawkins, Simon, Hongxing He, Graham Williams, and Rohan Baxter.” Outlier detection using replicator neural networks.” In International Conference on Data Warehousing and Knowledge Discovery, pp. 170-180. Springer, Berlin, Heidelberg, 2002.
31. Qiu, Juan, Qingfeng Du, and Chongshu Qian. ”Kpi-tsad: A time-series anomaly detector for kpi monitoring in cloud applications.” Symmetry 11, no. 11 (2019): 1350
32. Ho, Tin Kam.” Random decision forests.” In Proceedings of 3rd international conference on document analysis and recognition, vol. 1, pp. 278-282. IEEE, 1995.
33. Aggarwal, Charu C.” An introduction to outlier analysis.” In Outlier analysis, pp. 1-34. Springer, Cham, 2017.
34. Min-Seong Kwon, Yong-Geun Moon, Byungju Lee, Jung-Hoon Noh. "Autoencoders with Exponential Deviation Loss for Weakly Supervised Anomaly Detection", Pattern Recognition Letters, 2023
35. Charu C. Aggarwal. "Outlier Analysis", Springer Science and Business Media LLC, 2017
36. Alireza Vafaei Sadr, Bruce A Bassett, Emmanuel Sekyi. "Personalized anomaly detection using deep active learning", RAS Techniques and Instruments, 2023
37. Konstantinos Demestichas, Theodoros Alexakis, Nikolaos Peppes, Evgenia Adamopoulou. "Comparative Analysis of Machine Learning-Based Approaches for Anomaly Detection in Vehicular Data", Vehicles, 2021
38. Swethaa Prabhu, MV Sreenath, V Malavika, Himani Om, S Swetha. "Detection and Recognition of Animals Using Yolo Algorithm", 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2023
39. Hang Zhao, Yujing Wang, Juanyong Duan, Congrui Huang, Defu Cao, Yunhai Tong, Bixiong Xu, Jing Bai, Jie Tong, Qi Zhang. "Multivariate Time-series Anomaly Detection via Graph Attention Network", 2020 IEEE International Conference on Data Mining (ICDM), 2020
40. Mary Nankya, Robin Chataut, Robert Akl."Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies", Sensors, 2023
41. Gwanggil Jeon, Valerio Bellandi, Abdellah Chehri, Ernesto Damiani. "Deep learning approaches for vulnerable road users' safety", Safety Science, 2023
42. Sasho Nedelkoski, Jasmin Bogatinovski, Alexander Acker, Jorge Cardoso, Odej Kao. "Self-Attentive Classification-Based Anomaly Detection in Unstructured Logs", 2020 IEEE International Conference on Data Mining (ICDM), 2020
43. C. Jayaramulu, Bondu Venkateswarlu. "DLOT- Net: A Deep Learning Tool for Outlier Identification", 2022 6th International Conference on Electronics, Communication and Aerospace Technology, 2022
44. Ninh Pham, Rasmus Pagh. "A near-linear time approximation algorithm for angle-based outlier detection in high-dimensional data", Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, 2012
45. Jiangguo Liu, Jianli Gu, Huishu Li, Kenneth H. Carlson. "Machine learning and transport simulations for groundwater anomaly detection", Journal of Computational and Applied Mathematics, 2020
46. Min-Seong Kwon, Yong-Geun Moon, Byungju Lee, Jung-Hoon Noh. "Autoencoders with Exponential Deviation Loss for Weakly Supervised Anomaly Detection", Pattern Recognition Letters, 2023
47. Sudheer Hanumanthakari, Neha Garg, P Chandrakanth, Navdeep Dhaliwal, R Ramadevi, Siva Sankara Babu Chinka. "Deep Learning based Fault Diagnosis in Electrical Machinery in Industrial Sector based on Data Mining Techniques", 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), 2023
48. Daoheng Li, Xiushan Nie, Xiaofeng Li, Yu Zhang, Yilong Yin. "Context-related Video Anomaly Detection via Generative Adversarial Network", Pattern Recognition Letters, 2022
49. "ICAS 2021 Conference Proceedings [Front matter]", 2021 IEEE International Conference on Autonomous Systems (ICAS), 2021
50. Areej Alhothali, Amal Balabid, Reem Alharthi, Bander Alzahrani, Reem Alotaibi, Ahmed Barnawi. "Anomalous event detection and localization in dense crowd scenes", Multimedia Tools and Applications, 2022
51. Deepak T. Mane, Jyoti Mante, Anuradha Amar Bakare, Yatin Gandhi, Vinit Khetani, Rupali Atul Mahajan. "A Systematic Review on The Applications of Machine Learning for Fetal Birth Weight Prediction", Research Square Platform LLC, 2023
52. Gokul Yenduri, Dasaradharami Reddy K, Gautam Srivastava, Supriya Y, Ramalingam M, Thippa Reddy Gadekallu, Feras M. Awaysheh. "Federated Learning for the Metaverse: A Short Survey", 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), 2023
53. Haoyang Jia, Wenfen Liu. "Anomaly detection in images with shared autoencoders", Frontiers in Neurorobotics, 2023
54. S. Jayabharathi, V. Ilango. "Chapter 42 Anomaly Detection Using Machine Learning Techniques: A Systematic Review", Springer Science and Business Media LLC, 2023
55. Liunshun Zhao, Deke Guo, Junjie Xie, Lailong Luo, Yulong Shen. "A Closed-loop Hybrid Supervision Framework of Cryptocurrency Transactions for Data Trading in IoT", ACM Transactions on Internet of Things, 2022
56. Ufuk Bal, Alkan Bal, Özge Taylan Moral, Fatih Düzgün, Nida Gürbüz. "A deep learning feature extraction-based hybrid approach for detecting pediatric pneumonia in chest X-ray images", Physical and Engineering Sciences in Medicine, 2023

57. "Proceedings of Third International Conference on Communication, Computing and Electronics Systems", Springer Science and Business Media LLC, 2022
58. Hyunyong Lee, Nac-Woo Kim, Jun-Gi Lee, Byung-Tak Lee. "Patch-Level Operation with Adaptive Patch Control for Improving Anomaly Localization", IEEE Access, 2021
59. "Advances in Knowledge Discovery and Data Mining", Springer Science and Business Media LLC, 2018
60. Anubha Parashar, Apoorva Parashar, Weiping Ding, Mohammad Shabaz, Imad Rida. "Data preprocessing and feature selection techniques in gait recognition: A comparative study of machine learning and deep learning approaches", Pattern Recognition Letters, 2023
61. Keyu Chen, Guoping Zhao, Zhenfeng Yao, Zhihong Zhang. "Chapter 6 STAD: Multivariate Time Series Anomaly Detection Based onSpatio-Temporal Relationship", Springer Science and Business Media LLC, 2023
62. Ali Bou Nassif, Manar Abu Talib, Qassim Nasir, Fatima Mohamad Dakalbab. "MachineLearning for Anomaly Detection: A Systematic Review", IEEE Access, 2021
63. Haiqi Zhu, Seungmin Rho, Shaohui Liu, Feng Jiang. "Learning Spatial Graph Structure for Multivariate KPI Anomaly Detection in Large- scale Cyber-Physical Systems", IEEE Transactions on Instrumentation and Measurement, 2023
64. Md. Haidar Sharif, Lei Jiao, Christian W. Omlin. "Deep Crowd Anomaly Detection by Fusing Reconstruction and Prediction Networks", Electronics, 2023
65. Ning Li, Xue Liu, Ziyan Liu, Lin Mao, Lina Zhao, Xie Wang. "Anomaly Detection in Power Grid IoT System based on Isolated Forest", IEEE/WIC/ACM International Conference on Web Intelligence, 2021
66. Nomica Choudhry, Jemal Abawajy, Shamsul Huda, Imran Rao. "A Comprehensive Survey of Machine Learning Methods for Surveillance Videos Anomaly Detection", IEEE Access, 2023
67. Shivakumar R. Goniwada. "Introduction to Datafication", Springer Science and Business Media LLC, 2023
68. Armstrong Aboah, Maged Shoman, Vishal Mandal, Sayedomidreza Davami, Yaw Adu- Gyamfi, Anuj Sharma. "A Vision-based System for Traffic Anomaly Detection using Deep Learning and Decision Trees", 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2021
69. Mamoon M. Saeed, Rashid A. Saeed, Maha Abdelhaq, Raed Alsaqour, Mohammad Kamrul Hasan, Rania A. Mokhtar. "Anomaly Detection in 6G Networks Using Machine Learning Methods", Electronics, 2023
70. P. Valarmathi, G. Manoj, Sandip Kumar Das, Sujo Oommen, Mohit Tiwari. "Introduction and Development of Cyber Physical Systems in Smart Grid with Blockchain Technology to Enhance Sustainability", 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), 2023
71. Xuan Xia, Xizhou Pan, Nan Li, Xing He, Lin Ma, Xiaoguang Zhang, Ning Ding. "GAN-based Anomaly Detection: A Review", Neurocomputing, 2022
72. Yassine Himeur, Khalida Ghanem, Abdullah Alsalemi, Faycal Bensaali, Abbes Amira. "Artificial intelligence based anomaly detection of energy consumption in buildings: Exclude quotes Off Exclude Bibliography Off Exclude Matches Off A review, current trends and new perspectives", Applied Energy, 2021
73. Ahad Alloqmani, Yoosef B. Abushark, Asif Irshad Khan. "Anomaly Detection of Breast Cancer Using Deep Learning", Arabian Journal for Science and Engineering, 2023
74. Thittaporn Ganokratanaa, Supavadee Aramvith, Nicu Sebe. "Unsupervised Anomaly Detection and Localization Based on Deep Spatiotemporal Translation Network", IEEE Access, 2020
75. Zaheer, M. Z., Mahmood, A., Khan, M. H., Segu, M., Yu, F., & Lee, S. I. (2022). Generative Cooperative Learning for Unsupervised Video Anomaly Detection. arXiv preprint arXiv:2203.03962.