IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

Deep Learning Based Unsupervised Anomaly Detection of High Dimensional Time Series Data

Pritika Mehra[1], Mini Singh Ahuja[2]

Department of Computer Science and Engineering, Guru Nanak Dev University, Amritsar, India[1]

Department of Computer Science and Engineering, Guru Nanak Dev University Regional Campus, Gurdaspur, India [2]

ABSTRACT: In the context of COVID 19, on line commercial enterprise and on line training structures are unexpectedly changing offline work; the quantity of net customers is unexpectedly increasing in tandem with extra on line activities. Unusual incidents are happening everywhere in the global because of uncommon conditions. Organizations can be compelled to deal with their activity in a brand new ordinary because of those uncommon circumstances. As facts grow in length and dimension, it will become extra hard to identify anomalous events, particularly as misleading movements develop in quantity. As a result, Anomaly Detection is a urgent want in each industry. Anomaly detection is essential to save you corporations from collapsing because of fraud and antagonistic activity. Manual anomaly detection approaches have been utilised in the past, however manual detection of high dimensional datasets is difficult. As a result, automated anomaly detection techniques using statistical, data mining, and machine learning techniques have become increasingly common. Deep learning techniques have become increasingly popular in recent years. This study offers a thorough examination of deep learning approaches for high-dimensional time series datasets.

KEYWORDS: Anomaly, Anomaly Detection**,** deep learning, TCN, TCN-AE, Attention

I. INTRODUCTION

Anomaly detection is an essential research problem that has acquired a whole lot of interest in a number of fields. Anomaly detection is a subset of data mining that includes recognising matters or occurrences that don't comply with a predetermined pattern, in addition to different items in a dataset that might pass overlooked through a human expert. Such activities that deviate from their everyday behaviour are referred to as anomalies. Thus anomalies are items or activities that fluctuate from their ordinary behaviour. Anomalies may be transformed into problems consisting of structural flaws, faults, or frauds in general.

Anomaly

Something that deviates from typical behaviour or what is expected is referred to as an anomaly. A leaking connection pipe that causes the entire production line to shut down, multiple failed login attempts suggesting the likelihood of fishy cyber activity, and fraud detection in financial transactions are just a few examples of anomalies. Let's look at an example of a bank transaction for further clarification. Assume a user has a savings bank account from which he usually withdraws Rs 10,000, but one day he withdraws Rs 6, 00,000. This is a rare occurrence for the bank, as it usually deducts Rs 10,000 from the account. For bank staff, this transaction is unusual. The anomaly is a data observation that contradicts itself. It establishes that a particular model or assumption is incompatible with the issued statement. Point anomaly, contextual anomaly, and collective anomaly are the three types of anomalies.

Point Anomaly

A point anomaly occurs when a single instance in a dataset differs from the others in terms of its properties. In other words, when a specific value inside a dataset is unexpected in comparison to the rest of the data, this is referred to as a Point Anomaly. The above-mentioned example of the bank transaction is an example of point anomaly.

Contextual Anomaly

When the occurrence of data is anomalous for certain set of conditions, then it is known as Contextual Anomaly. For instance, the anomaly happens at a specified time interval. Thus the Contextual anomaly occurs when data is abnormal in a certain context.

These anomalies, also known as conditional anomalies, have values that differ dramatically from the values of other data points in the same context. In some cases, an anomaly in one dataset may not be an abnormality in another.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

Because time series datasets contain records of specified quantities over a period of time, outliers are typical. Although the value is consistent with global expectations, it may appear unusual in particular seasonal data patterns.
Contextual outliers are events that fall within the typical range on a global scale yet are out of the ordinary when seen in the context of seasonal cycles. It would be regarded a contextual abnormality if a customer only spends $2500 on gifts in December yet charges $2000 in July. While the expenditures for that month are within their normal global range, they occur at an exceptional period.

Collective Anomaly
A combination of multiple incidents can lead to the formation of collective anomalies. When a collection of occurrences of data is aberrant in comparison to the rest of the dataset then it is called collective anomaly. In other words, when a subset of data points within a set deviates from the norm for the entire dataset, those values are referred to as collective outliers. Individual values in this category are not out of place globally or contextually. When we examine different time series together, we start to notice these types of anomalies. Individual behaviour in a specific time series dataset may not deviate from the normal range. When combined with another time series dataset, however, more significant anomalies emerge.

Breaking the trend observed in ECG is an example of collective anomaly. Collective anomalies are events that, on their own, do not deviate from the expected pattern of behaviour, but when combined, represent an anomaly. A group of customers with a history of order cancellations cancelling their orders all at the same time would be considered a collective anomaly.

As soon as possible, anomalies should be distinguished from the typical pattern. To provide real-time notifications, anomaly detection should be done on streaming data. Some anomalies are uninteresting, but others are critical. As an example, An irregularity that directly affects revenue may be more serious than one that affects engagement. A steady metric anomaly may be more intriguing than a dynamic metric anomaly. Anomalies of a larger size are more likely to be fascinating than those of a smaller size. Thus Anomalies are just variations from the expected value for a metric at any particular point in time; they aren't categorically good or bad. Thus Anomaly detection is a useful tool for detecting unusual events that may have great significance but are difficult to find.

II. HIGH DIMENSIONAL TIME SERIES DATA

High Dimensional denotes that there are a dizzying amount of dimensions – so many that computations become incredibly complex. The number of features in high-dimensional data can outnumber the number of observations. The present tendency is for more observations, but even more so for a large number of features. Curves, photographs, and movies might constitute the observations, with each having thousands, millions, or billions of dimensions but just tens or hundreds of observations to study. This is referred to as High Dimensional Data. Microarrays, for example, which monitor gene expression, can have hundreds or thousands of samples. Thousands of genes can be found in a single sample. There are millions of potential gene combinations in a single individual (i.e. one observation). Other industries where features outnumber observations and high-dimensional data can be employed include finance, high-resolution photography, biometrics, medical, e-commerce, network security, industrial applications, and website analysis (e.g. advertising, crawling, or ranking). Combining high dimensionality with large datasets can be extremely difficult and demanding. Correct methodologies and methods for dealing with such high-dimensional data must be used to utilise data features. Furthermore, data can have distinct properties and complex data structures, rendering typical analysis methods worthless. To extract additional useful information from high-dimensional data, new approaches are necessary. A time series is a collection of data that associates each value with a certain time period. Any measurable quantity that is time dependent in some way, such as pricing, humidity, or the number of people, can be used as the value.

Time Series Anomaly Detection
Time series data anomaly detection is concerned with data that change over time. On our own computer, for example, CPU consumption, network usage, memory usage, and other factors change over time. You can graph it as a line graph on the X-axis and time on the Y-axis. It clearly depicts the evolution of the metric over time. Time series anomaly detection is the process of understanding the behaviour of time series data using AI/ML algorithms and then detecting any unexpected behaviour, such as a sudden spike or dip.
Time series data is made up of a series of values that change over time. That is, each point is typically composed of two items: a timestamp for when the metric was measured and the value associated with that metric at the time.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

III. ANOMALY DETECTION METHODS

Manual

Manual anomaly detection was once a feasible method for detecting anomalies by hand in the past. One simply needed to measure a few Key Performance Indicators throughout the organization, and the datasets were small enough for an analytics team to handle. However, we now have access to more data than ever before, and thus traditional, manual anomaly detection has one major flaw: it doesn't scale to large number of metrics. When there are hundreds, thousands, or even millions of metrics to handle, manual anomaly detection becomes impossible. It is tedious to perform anomaly detection by hand. This requires domain knowledge and—even more difficult to access—foresight.

Manual detection methods would introduce inconsistencies and human error. Tracking a large number of metrics necessitates the hiring of a large team of staff members. For example, if one person can perform anomaly detection for 100 metrics at once, then 10,000 or more people would be required just for anomaly detection for 1 million or more metrics. It is practically impossible to hire such a large number of people in an organisation solely for the purpose of detecting anomalies. There's a limit to how many people an organization can hire, how much experience they can provide, and how accurate their anomaly detection insights can be.

Manual anomaly detection in real-time is very challenging, time consuming and expensive.

Automated Anomaly Detection

Because manual anomaly detection is currently impractical, automated anomaly detection which is adaptable and timely, and can handle large datasets is used. Keeping the current situation in mind necessitates automated anomaly detection that can provide accurate, real-time insights regardless of how many metrics one needs to track. True automated anomaly detection systems should detect, rank, and group data, removing the need for large teams of analysts.

The following are some of the ways that an automated anomaly detection system might benefit an organization:

- It connects to all of the various data sources from which the metrics are derived.
- It employs patented unsupervised algorithms that are designed to comprehend and learn all of the data's trends, periodicity, and seasonality.
- It can autonomously identify all emergent issues that depart from usual behaviour in real time.
- Different anomalies can be categorised using correlation, which can help with root cause analysis in the event of an occurrence.
- It gives Smart Insights that business customers can consume without the need for data experts.
- It saves time and effort in configuration and development, allowing the Company to concentrate on the results and make informed decisions.

Types of Automated Anomaly Detection Methods for High Dimensional Time Series

Anomalies in input data can be identified using a variety of automated model-based methods. They are detected using a variety of tools and approaches, ranging from simple statistical techniques to complicated machine learning and deep learning algorithms, depending on the complexity of the data and the level of sophistication required. The computational approaches for anomaly detection of time series can be divided into three categories, according to prior studies published in the literature:

I. Statistical methods
II. Data Mining based techniques
III. Classical machine learning methods

Statistical methods

There are some simple but effective statistical tools that can be used to screen anomalies quickly. While the employment of sophisticated algorithms is occasionally unavoidable, sometimes simple techniques are sufficient. Anomaly detection can be done using a variety of statistical approaches such as the Z-score, IQR, Histogram, and BOXPLOT. Given the enormous number of input variables, identifying and removing anomalies with simple statistical methods is difficult for large datasets. For many years, statistical-based models such as Autoregressive Model(AR), Moving Average Model (MA), Autoregressive Moving Average Model (ARMA), Autoregressive integrated moving

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

average,(ARIMA), and others were the state-of-the-art for detecting anomalies in time series [1]. [2] specified Gaussian mixture model, Regression model, and Histogram Based Outlier detection (HBOS) algorithm for anomaly detection. A disadvantage of these methods is that anomaly identification is dependent on the assumption that data is collected using a specific statistical distribution [2].

Data Mining Based Techniques

The literature contains data mining techniques such as clustering and classification. Researchers have primarily employed K-means clustering to group similar data points and data points outside of these clusters have been regarded as anomalies. These methods function in an unsupervised mode; nevertheless, with smaller datasets, they may not provide reliable insights at the appropriate degree of detail. Anomaly detection has been successfully applied using data mining approaches such as Subsequence Time-Series Clustering (STSC), Density-Based Spatial Clustering of Applications with Noise (DBSCAN), Isolation Forest, One-Class Support Vector Machines (OC-SVM), and others [1].

Machine Learning Methods

In recent years, Machine learning methods have been shown to boost performance in anomaly detection problems. Machine learning can be used to learn a system's properties from observed data, which can help to improve detection speed. Machine-learning algorithms are capable of not only learning from data, but also making predictions based on that data, as well as improving their predictive abilities by "learning" from the outcomes of their initial predictions as events unfold in real life (the feedback loop). Machine learning techniques for anomaly detection include methods for detecting and classifying anomalies in vast and complex big data sets. The traditional machine learning (ML) techniques are suboptimal when it comes to high-dimensional data and sequence datasets, because they fail to capture the complex structures in the data. Machine learning techniques include fuzzy logic, genetic algorithm, Bayesian approach and neural network [2].

Supervised Machine Learning

To build a prediction model, the supervised technique requires a labelled training set with normal and anomalous observations. Supervised neural networks, support vector machines, k-nearest neighbours, Bayesian networks, and decision trees are some of the most common supervised approaches.

Because of their ability to include both previous knowledge and data and produce a confidence score with the model output, supervised models are thought to have a greater detection rate than unsupervised methods. In actuality, this isn't always the case because anomalies come in a variety of shapes and sizes, with new abnormalities arising during testing. As a result, unsupervised methods that generalise well and are more successful at detecting previously undetected anomalies are preferred.

Unsupervised Machine Learning

Unsupervised approaches do not require training data that has been manually labelled. They assume that the majority of the data is normal, with only a small percentage of it being abnormal, and that malicious data will be statistically distinct from regular data. Based on these two assumptions, data groups with many comparable examples are considered normal, while data groups with few similar instances are classified as harmful.

K-means, Autoencoders, (Gaussian Mixture Modelling) GMMs, PCAs (Principal Component Analysis), and hypothesis tests-based analysis are some of the most prominent unsupervised algorithms.

Because of the lack of labelled data, supervised algorithms are not appropriate for time series data. As a result, for anomaly detection, unsupervised algorithms are used. Unsupervised Learning is a subfield of Anomaly Detection, which is a broader research field.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

Limitations of Machine Learning Approaches

- The gathering of data is one of the most unpleasant aspects of Machine Learning. When we collect data through surveys, there is a chance that it will contain a considerable amount of fake and erroneous information. We frequently encounter situations in which data is unbalanced, resulting in low model accuracy. Because of these factors, data gathering is a significant disadvantage of Machine Learning.
- Machine Learning models can process enormous volumes of data. The more data there is, the longer it takes to learn from it and interpret it. It could also mean more computational resources in some cases.

Therefore, there is a shift from machine learning to deep learning due to the limits of machine learning approaches.

Deep learning (DL) approaches, as a branch of machine learning, hold a lot of potential over classical machine learning, with improved accuracy, greater flexibility, stronger generalisation, and less reliance on domain expertise.

IV. DEEP LEARNING

The shift from Machine Learning to Deep Learning approaches is a recent development. Deep learning (DL) has lately gained popularity as a highly effective method for detecting time series anomalies. Due to its ability to extract complicated patterns automatically without the need for feature extraction pre-processing, DL models are particularly well suited to high-dimensional temporal sequences. LSTM (Long Short-Term Memory), Autoencoders, MLP (Multilayer Perceptron), GAN (Generative Adversarial Network), and other deep learning methods are available. In the time series anomaly detection sector, more specialised DL models such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) began to gain attention. It is extremely difficult to train an RNN. When using tanh or relu as an activation function, it cannot process very long sequences. However, the CNN's basic flaws, such as its fixed-size input vector and inconsistent input and output sizes, restrict its use in time-series. Therefore, a specific CNN architecture known as Temporal Convolutional Network (TCN) has recently gained popularity due to its suitability for dealing with time series data. [3] were the first to propose the concept of TCN. It was created to analyse long-term sequences. The primary characteristics of Temporal Convolutional Network for complex time series problems are:

- TCNs have the advantage of being able to handle variable-length inputs, similar to RNNs.
- TCNs also use less memory than recurrent networks because of their shared convolution architecture, which enables them to analyse large sequences in parallel. The input sequences in RNNs are processed sequentially, resulting in a longer computation time [4].
- TCNs are also trained using the normal back propagation technique, which avoids the gradient difficulties associated with the RNN's back propagation-through-time approach (BPTT).
- The output size is equal to the input size (we can keep the sequence length as in a recurrent neural network);
- No future information is taken into account for the characteristics from step t, which can be ensured by using a causal convolution;
- The dilation factor is used for causal convolutions to ensure a large receptive field.
- TCNs can extract long-term patterns utilising dilated causal convolutions and residual blocks, and they are also more computationally efficient [4].

The TCN has a basic network structure and beats traditional recurrent networks like the recurrent neural network (RNN) and Convolutional neural network (CNN) in terms of time-series data analysis accuracy and efficiency [5].

TCN has greater detection accuracy, however when doing data processing; this technique often separates the data into blocks in an overly simplified manner. When a data block is used as a distinct vector input model, the data's correlation can be lost [6]. Therefore, TCN can be combined with Autoencoder to overcome this limitation for detection of anomalies.

TCN with Autoencoder is introduced in the literature for anomaly detection in time series [6] and [7]. Autoencoders are supplementary neural networks that help with data cleansing, denoising, feature extraction, and dimensionality reduction when used in conjunction with machine learning models. Autoencoders are a method for detecting anomalies

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

based on unsupervised approach. When dealing with complex and non-linear data problems, autoencoder approaches show their worth.

V. CONCLUSION

Deep learning algorithms have recently been employed for anomaly detection. Deep learning techniques include LSTM, Autoencoders, MLP, GAN, RNN, CNN, TCN, and TCN-AE. TCN-AE can be expanded in the future to improve the efficiency and performance of the anomaly detection system.

REFERENCES

1. M. Braei and S. Wagner, "Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art," 2020, [Online]. Available: http://arxiv.org/abs/2004.00433.
2. Z. Ji, J. Gong, and J. Feng, "A Novel Deep Learning Approach for Anomaly Detection of Time Series Data," *Sci. Program.*, vol. 2021, 2021, doi: 10.1155/2021/6636270.
3. C. Lea, M. D. F. Ren, A. Reiter, and G. D. Hager, "Temporal Convolutional Networks for Action Segmentation and Detection," pp. 156–165, 2016, [Online]. Available: https://arxiv.org/pdf/1611.05267.pdf.
4. P. Lara-Benítez, M. Carranza-García, J. M. Luna-Romera, and J. C. Riquelme, "Temporal convolutional networks applied to energy-related time series forecasting," *Appl. Sci.*, vol. 10, no. 7, pp. 1–17, 2020, doi: 10.3390/app10072322.
5. J. Yan, L. Mu, L. Wang, R. Ranjan, and A. Y. Zomaya, "Temporal Convolutional Networks for the Advance Prediction of ENSO," *Sci. Rep.*, vol. 10, no. 1, pp. 1–15, 2020, doi: 10.1038/s41598-020-65070-5.
6. C. Meng, X. S. Jiang, X. M. Wei, and T. Wei, "A Time Convolutional Network Based Outlier Detection for Multidimensional Time Series in Cyber-Physical-Social Systems," *IEEE Access*, vol. 8, pp. 74933–74942, 2020, doi: 10.1109/ACCESS.2020.2988797.
   M. Thill, W. Konen, H. Wang, and T. Bäck, "Temporal convolutional autoencoder for unsupervised anomaly detection in time series," *Appl. Soft Comput.*, vol. 112, p. 107751, 2021, doi: 10.1016/j.asoc.2021.107751.
7. Chandola V., Banerjee A., Kumar V., Anomaly detection:A survey, ACM Computing Surveys (CSUR); 41(3);2009; p.15
8. Agrawal S.,Agrawal J., Survey on Anomaly detection using data mining techniques, Procedia Computer Science 60; 2015; p.708-713
9. Blomquist H., Miller J., Anomaly detection with machine learning; Examinator; 2015; 1650-8319;UPTEC STS15 014
10. Goldstein M., Uchida S., A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data, PLOS ONE 11(4);2016; doi: 10.1371/ journal.pone.0152173
11. Habeeb R., Gani A., Nasaruddin F., Hasheem I., Real time big data processing for anomaly detection: A survey; doi:10.1016/j.ijinfomgt; 2018.08.006
12. Raghavendra Chalapathy, Sanjay Chawla, Deep Learning for Anomaly Detection-A survry; arXiv:1901.03407v2, 2019
13. Xiodan Xu, Huawen Liu, Minghai Yao, Recent progress of anomaly detection Hindawi; Complexity; 2019;2686378
14. Thudumu, S., Branch, P., Jin, J. *et al.* A comprehensive survey of anomaly detection techniques for high dimensional big data. *J Big Data* **7,** 42 (2020). https://doi.org/10.1186/s40537-020-00320-x
15. Karadayı Y, Aydin MN, Öğrenci AS. A Hybrid Deep Learning Framework for Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data. *Applied Sciences*. 2020; 10(15):5191. https://doi.org/10.3390/app10155191
16. Amarbayasgalan T, Pham VH, Theera-Umpon N, Ryu KH. Unsupervised Anomaly Detection Approach for Time-Series in Multi-Domains Using Deep Reconstruction Error. *Symmetry*. 2020; 12(8):1251. https://doi.org/10.3390/sym12081251
17. https://towardsdatascience.com/a-brief-overview-of-outlier-detection-techniques-1e0b2c19e561
18. https://towardsdatascience.com/effective-approaches-for-time-series-anomaly-detection -9485b40077f1
19. https://towardsdatascience.com/unsupervised-learning-for-anomaly-detection-44c55a96b8c1
20. https://towardsdatascience.com/unsupervised-anomaly-detection-on-time-series-9bcee10ab473
21. Xiaodan Xu , Huawen Liu , Li Li , Minghai Yao, A Comparison of Outlier Detection Techniques for High-Dimensional Data, International Journal of Computational Intelligence Systems, Vol. 11 (2018) 652–662
22. Ane Blazquez-Garcia and Angel Conde, et. al.,A review on outlier/anomaly detection in time series data, arXiv:2002.04236v1, ACM ,2020

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912025 |

23. Lary Shoemaker, Lawrence O Hall, MCS'11: Proceedings of the 10th international conference on Multiple classifier systemsJune 2011 Pages 6–15
24. Shweta B. Meshram, Sharmila M. Shinde, A Survey on Ensemble Methods for High Dimensional Data Classification in Biomedicine Field, International Journal of Computer Applications (0975 – 8887) Volume 111 – No 11, February 2015
25. Priyanga Dilini Talagala, Rob J. Hyndman, Kate Smith-Miles, 2019, arXiv:1908.04000
26. https://365datascience.com/tutorials/time-series-analysis-tutorials/time-series-data/
27. Tung Kieu , Bin Yang, Chenjuan Guo and Christian S. Jensen, Outlier Detection for Time Series with Recurrent Autoencoder Ensembles,Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI-19).
28. Narendhar Gugulothu, Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, Sparse Neural Networks for Anomaly Detection in High-Dimensional Time Series, International Workshop on AI for Internet of Things, IJCAI 2018, Stockholm, Sweden.
29. Nadeem Iftikhara, Thorkil Baattrup-Andersenb, Finn Ebertsen Nordbjerga, Karsten Jeppesena, Outlier Detection in Sensor Data using Ensemble Learning, Procedia Computer Science 176 (2020) 1160–1169
30. Peter Goldthorpe, Antoine Desmet, Denoising autoencoder anomaly detection for correlated data, EUROPEAN CONFERENCE OF THE PROGNOSTICS AND HEALTH MANAGEMENT SOCIETY 2018
31. Yeldız Karadayı , Mehmet N. Aydin and A. Selçuk Ö ˘grenci, A Hybrid Deep Learning Framework for Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data, Appl. Sci. 2020, 10, 5191; doi:10.3390/app10155191, 2020
32. Lukas Ruff, Jacob R. Kauffmann, Robert A. Vandermeulen, Gregoire Montavon, Wojciech Samek, ´ Marius Kloft, Thomas G. Dietterich, Klaus-Robert Muller, A Unifying Review of Deep and Shallow Anomaly Detection , arXiv:2009.11732v2, 2020
33. Zheng Gao, Lin Guo, Chi Ma, Xiao Ma, Kai Sun, Hang Xiang, Xiaoqiang Zhu, Hongsong Li, Xiaozhong Liu, AMAD: Adversarial Multiscale Anomaly Detection on High-Dimensional and Time-Evolving Categorical Data, arXiv:1907.06582v1, 2019
34. Chao Meng , Xue Song Jiang , Xiu Mei Wei , And Tao Wei, A Time Convolutional Network Based Outlier Detection for Multidimensional Time Series in Cyber-Physical-Social Systems, 10.1109/ACCESS.2020.2988797
35. Arnav Kundu, Abhijeet Sahu, Erchin Serpedin and Katherine Davis, A3D: Attention-based Auto-encoder Anomaly Detector for False Data Injection Attacks, Electric Power Systems Research. 189. 106795. 10.1016/j.epsr.2020.106795
36. Zhao, Zhiruo, "Ensemble Methods for Anomaly Detection" (2017). Dissertations - ALL. 817. https://surface.syr.edu/etd/817
37. Maya, S., Ueno, K. & Nishikawa, T. dLSTM: a new approach for anomaly detection using deep learning with delayed prediction. *International Journal of Data Science Anal*ysis **8,** 137–164 (2019). https://doi.org/10.1007/s41060-019-00186-0
38. Sen, Rajat & Yu, Hsiang-Fu & Dhillon, Inderjit, Think Globally, Act Locally: A Deep Neural Network Approach to High-Dimensional Time Series Forecasting, Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, 8-14 December 2019, Vancouver, BC, Canada. pages 4838-4847, 2019.
39. Pereira, João. (2018). Unsupervised Anomaly Detection in Time Series Data using Deep Learning. 10.13140/RG.2.2.15967.07849.
40. https://ff12.fastforwardlabs.com/
41. https://www.xenonstack.com/blog/time-series-deep-learning.
42. https://neptune.ai/blog/anomaly-detection-in-time-series
43. https://www.intechopen.com/chapters/58448
44. https://www.statisticshowto.com/dimensionality/
45. https://towardsdatascience.com/statistical-techniques-for-anomaly-detection-6ac89e32d17a
46. http://ivyproschool.com/blog/advantages-and-disadvantages-of-machine-learning-in-2020/
47. https://purnasaigudikandula.medium.com/recurrent-neural-networks-and-lstm-explained-7f51c7f6bbb9

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details