Literature Review of Anomaly Detection on Time Series Data

D1.1

Authors:

Onur Enginar (Presify)

Ömer Aynur (Presify)

Rabia Şeyma Güneş (Presify)

Verified by the appointed Reviewers	Dmitry Belichenko (ENTSO-E), 27.01.2023
Dissemination Level	Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	19.12.2022
Actual date of delivery	16.01.2023
Status and version	1.1

Version	Date	Author(s)	Notes
1.0	16.12.2022	Onur Enginar, Ömer Aynur, Rabia Şeyma Güneş	
1.1	16.01.2023	Onur Enginar, Ömer Aynur, Rabia Şeyma Güneş	Conclusion was added. Table of contents was updated. Reviewer’s comments addressed.

Disclaimer:

All information provided reflects the status of the OneNet project at the time of writing and may be subject to change. All information reflects only the author’s view and the European Climate, Infrastructure and Environment Executive Agency (CINEA) is not responsible for any use that may be made of the information contained in this deliverable.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

About OneNet

OneNet will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

The project OneNet (One Network for Europe) is funded through the EU's eighth Framework Programme Horizon 2020. It is titled "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

While the electrical grid is moving from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. For this reason, the two major associations of grid operators in Europe, ENTSO-E and EDSO, have activated their members to put together a unique consortium.

OneNet will see the participation of a consortium of over 70 partners. Key partners in the consortium include: already mentioned ENTSO-E and EDSO, Elering, E-REDES, RWTH Aachen University, University of Comillas, VITO, European Dynamics, Ubitech, Engineering, and the EUI's Florence School of Regulation (Energy).

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
LDR	Local Density Ratio
LOF	Local Outlier Factor
ML	Machine Learning
SVD	Support Value Decomposition

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Executive Summary

This document provides a detailed literature review of anomaly detection for time series data. First of all, the nature of anomalies is examined, and then types of anomalies such as point, contextual and collective are explained. So main focus point is on time series data, and structures of all statistical and machine learning-based methods for anomaly detection on time series data are included. Especially, the candidate models for base models of the ensemble model, which will be developed in this project, are explained in detail.

1 Introduction

While current machine learning research more focused on models; data, which have been used in these models, are usually overlooked. However, data quality plays a key role on model accuracy. Recently, data centric ai, which basically tries to improve data to improve model accuracy in contrast to model centric ai, has started to receive attention from both in academia and industry[12].

There are many ways to improve datasets. Data preprocessing is a crucial step before model training by cleaning and transforming data which improves data. One of the first research by researchers[3] on data cleansing method proposes manually finding the patterns and cleansing the data accordingly. Further data cleaning algorithms proposed by various researchers on removing biases[4] or spurious correlations from train set[5]. Data cleaning deals with missing and noisy data and outliers and anomalies as well. In particular, anomalies and outliers are often used interchangeably. The problem of finding patterns in data that do not conform to expected or normal behavior is referred as anomaly detection.[6] There are many areas that anomaly detection is being widely used: detecting network attacks[7]; medical image[8]; credit card fraud detection – identity theft[9] detecting anomalies in space craft sensor readings[10]; mobile cellular network fraud; intrusion detecting.

Anomalies are often divided into point and pattern anomalies. Point anomalies are individual single deviation from systems expected behavior. On the other hand, pattern anomalies are multiple deviations that collectively deviate from systems expected behavior**.** A contextual anomaly is also known as the conditional anomaly is a data instance that could be considered as anomalous in some specific context.[11]

[1] https://landing.ai/data-centric-ai/

[2] https://datacentricai.org/

[3] Isabelle Guyon, Nada Matic, Vladimir Vapnik, et al. Discovering informative patterns and data cleaning., 1996.

[4] Tommasi, T., Patricia, N., Caputo, B., & Tuytelaars, T. (2017). A deeper look at dataset bias. In Domain adaptation in computer vision applications (pp. 37-55). Springer, Cham.

[5] Abedjan, Z., Chu, X., Deng, D., Fernandez, R.C., Ilyas, I.F., Ouzzani, M., Papotti, P., Stonebraker, M., Tang, N.: Detecting data errors: Where are we and what needs to be done? Proc. VLDB Endow. 9(12), 993–1004 (Aug 2016). https://doi.org/10.14778/2994509.2994518

[6] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), 1-58.

[7] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), 1-58

[8] Spence, C., Parra, L., and Sajda, P. 2001. Detection, synthesis and compression in mammographic image analysis with a hierarchical image probability model. In Proceedings of the IEEE Workshop on Mathematical Methods in Biomedical Image Analysis. IEEE Computer Society, 3

[9] Aleskerov, E., Freisleben, B., and Rao, B. 1997. Cardwatch: A neural network based database mining system for credit card fraud detection. In Proceedings of the IEEE Conference on Computational Intelligence for Financial Engineering. 220--226

[10] Fujimaki, R., Yairi, T., and Machida, K. 2005. An approach to spacecraft anomaly detection problem using kernel feature space. In Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. ACM Press, 401--410.

[11] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

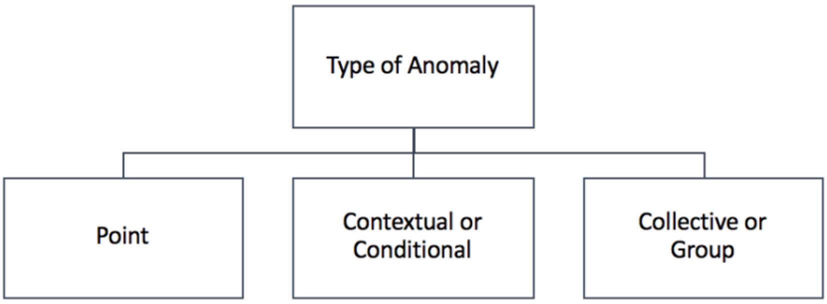


Figure 1.1: Type of Anomalies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2 Content

2.1 Time Series Anomaly Detection

Data recorded over chorological time index is known as time series. Being recorded over chorological time index is the differentiating point of time series data from other datasets. Time series data could be both univariate and multivariate which contains multiple variables recorded over same period while univariate time series has a single variable. Time series anomaly detection concerns with identifying the anomalies in a time series datasets[12].

2.2 Anomaly Detection Techniques

Depending on label availability, we can consider anomalies detection methods as supervised where deviations are labeled as anomaly; unsupervised where there are no labeled data instances as anomaly; and semi-supervised where we can benefit from both supervised and unsupervised methods. Unsupervised methods have advantages over supervised methods, since no anomaly labels is needed, which is cost-saving and more flexible. Unsupervised methods are dominated with clustering-based approach which basically divides dataset into regular and anomaly points.

Based on methodology, anomaly detection techniques could be divided as statistical and machine learning anomaly detection. In this section, we review different methods have been used in anomaly detection. It is important to note that, there are several challenges with anomaly detection regarding both statistical and machine learning anomaly detection, such as lack of labels (available labelled data), model generalization and efficiency[13].

2.2.1 Anomaly Detection with Statistical Methods

Statistical anomaly detection is widely studied in literature. In general, statistical anomaly detection concerns with a particular difference metric based on real data and statistical model or statistical distribution output[14]. The latter deals with assign a distribution and then the anomaly is found by checking whether data complies with this distribution. There are several other methods used in literature, including hypothesis testing[15]; SVD

[12] H. -S. Wu, "A survey of research on anomaly detection for time series," 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2016, pp. 426-431, doi: 10.1109/ICCWAMTIP.2016.8079887.

[13] Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., & Zhang, Q. (2019, July). Time-series anomaly detection service at microsoft. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* (pp. 3009-3017).

[14] Chandola. V, Banerjee. A, Kumar. V, "Anomaly Detection: A Survey", ACM Computing Surveys, Vol.41, No.3, pp. 1-58, Nov, 2009

[15] Percentage points for a generalized ESD many-outlier procedure. Technometrics 25, 2 (1983), 165–172.

and auto-regressive integrated moving average (ARIMA) models[16]; Holt-Winters[17]; Wavelet analysis[18]; Fourier Transform[19]; extreme value theory[20]. In general, studies in literature aims to model data generation process with statistical models to assess anomaly.

2.2.2 Anomaly Detection with Machine Learning

Machine learning based anomaly detection simply uses various machine learning models to represent data generation process and then assess anomaly. Both machine and deep learning models are used in literature. Unsupervised models are in general dominated with clustering methods which based on generating a cluster which contains anomaly points in[21]. Rest of this part is based on supervised machine learning models such as Bayesian models[22]; Support vector machines[23]; K-Nearest Neighbors[24], tree-based models (decision trees)[25] . There are also deep learning-based anomaly detection models in literature as well. Feed forward neural network models[26] [27]; convolution neural networks which are frequently used in image processing[28].

2.2.3 Candidate Models

[16] Ajay Mahimkar, Zihui Ge, Jia Wang, Jennifer Yates, Yin Zhang, Joanne Emmons, Brian Huntley, and Mark Stockert. 2011. Rapid detection of maintenance induced changes in service performance. In Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies. ACM, 13.

[17] Holt-Winters forecasting Procedure. Journal of the Royal Statistical Society, Applied Statistics 27, 3 (1978)

[18] Wei Lu and Ali A Ghorbani. 2009. Network anomaly detection based on wavelet analysis. EURASIP Journal on Advances in Signal Processing 2009 (2009), 4.

[19] Faraz Rasheed, Peter Peng, Reda Alhajj, and Jon Rokne. 2009. Fourier transform based spatial outlier mining. In International Conference on Intelligent Data Engineering and Automated Learning. Springer, 317–324.

[20] Alban Siffer, Pierre-Alain Fouque, Alexandre Termier, and Christine Largouet. 2017. Anomaly detection in streams with extreme value theory. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 1067–1075.

[21] LI,H 2010.Research and Implementation of an Anomaly Detection Model Based on Clustering Analysis. International Symposium on Intelligent Information Processing and Trusted Computing

[22]Moore, D.2005. Internet Traffic Classification Using Bayesian Analysis Techniques. in Proceedings of ACM SIGMETRICS.; Johansen, K. and Lee. ” CS424 network security: Bayesian Network Intrusion Detection (BINDS)”: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1 .83.8479

[23] Mukkamala,S.,Sung, A.and Ribeiro, B.2005. Model Selection for Kernel Based Intrusion Detection Systems. Proceedings of International Conference on Adaptive and Natural Computing Algorithm.

[24] Ming, Y. 2011. Real Time Anomaly Detection Systems for Denial of Service Attacks by Weighted k-NearestNeighbor Classifiers”. Expert Systems with Applications, Vol.38, 2011, pp. 3492-3498.

[25] Peddabachigari, S., Abraham, A., Grosan, C. and Thomas, J. 2007.” Modeling Intrusion Detection System using Hybrid Intelligent Systems”. J. Netw. Comput. Appl, Vol. 30, NO1, PP. 114-132.

[26] Sangmin Lee, Hak Gu Kim, and Yong Man Ro. Stan: Spatio-temporal adversarial networks for abnormal event detection. arXiv preprint arXiv:1804.08381, 2018.

[27] MATE SZEKER. Spatio-temporal outlier detection in streaming trajectory data, 2014.

[28] Donghwoon Kwon, Kathiravan Natarajan, Sang C Suh, Hyunjoo Kim, and Jinoh Kim. An empirical study on network anomaly detection using convolutional neural networks. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pages 1595–1598. IEEE, 2018.

In this section we investigate in detail, various anomaly detection models which we aim to use in this project as base models:

2.2.3.1 Autoencoders

An autoencoder is a machine learning model that takes in data and tries to recreate it using multiple hidden layers. This process of reconstruction allows the autoencoder to learn the underlying structure of the data and create a compact representation of it in the hidden layers. When trained on normal data, an autoencoder will be able to recreate the input data accurately. However, when presented with anomalous or outlier data, the autoencoder will be unable to recreate it accurately, resulting in a large error or residual. This difference in the ability to recreate normal versus anomalous data can be used to identify and flag outliers in a dataset.

2.2.3.1.1 Deep ensemble autoencoder

Recently, Recurrent neural networks are subclass of deep learning models that performing superior in sequential learning problems gained popularity among scholars in anomaly detection. It could capture both long term and short-term dependencies in sequential data and therefore predicts it accurately. Recurrent autoencoders models are models that constructs time series and its embeddings via encoder and decoder structure, where encoder generates embeddings and decoder reconstructs series via encoded embeddings. Thereby, natural behavior of time series could be detected via this autoencoder, and anomalies could be detected as divergence from expected behavior of time series represented by recurrent autoencoder. However, a single autoencoder might not sufficiently capture the nature of time series due to noisiness of time series data. To tackle this problem deep ensembles emerges. Power of ensembling methods is due to diversity by initializing randomly parameters of each neural network in the ensemble or bootstrapping the dataset. Deep ensembles combine N models, which are called base models, generally by simple averaging it exploits the correlations between those models and generate more robust predictor. Moreover, deep ensemble models are capable of approximating distribution of predictions by which anomaly detection could be performed. Using these predictive intervals, anomaly could be detected easily just by calculating the distance of potential anomaly point from upper and lower intervals.

Pros and Cons:

- Unsupervised, does not need labeled data
- Works well with big data.
- Model training could be expensive

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2.2.3.2 Local Outlier Factor

LOF algorithm is unsupervised method to find outliers in dataset. It aims to compute the local density deviation of given data point with respect to its neighbors. It considers as outliers the points which have substantially lower density than their neighbors.[29] The goal of the LOF algorithm is to capture the spirit of local outliers rather than global outliers which is often harder to succeed. LOF algorithm is applied to many diverse types of time series datasets to identify the anomalies. In [30] LOF outperforms many other anomaly detection algorithms in terms of accuracy and False Positive rates. Other work[31] proved that the LOF algorithm is highly performant in capturing unique events in a time series dataset.

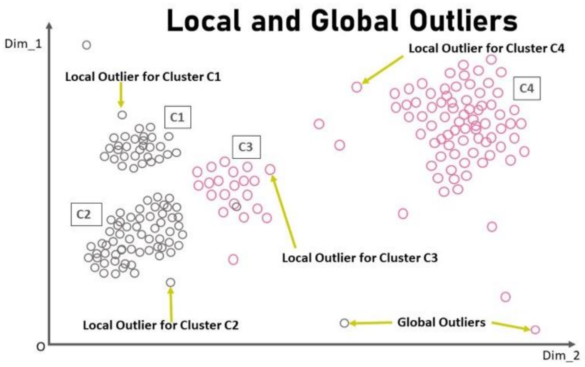


Figure 2.1: The Structure of Local Outlier Factor

Algorithm:

For a given dataset,

$$D_n = \{(x_i, y_i) | x_i \in R^2, y_i \in \{X, Y, Z\}\}$$

Then, local outlier factor for each data point is given by:

$$LOF(x_i) = \frac{\sum_{\{x_j \in N(x_i)\}} lrd(x_j)}{|N(x_i)|} x(\frac{1}{lrd(x_i)})$$

where $|N(x_i)|$: number of elements in the neighborhood of $x_i$and $lrd(x_i)$: local reachability density of x_i.

As diagram above illustrate Local Outlier Factor is sum of LDR of all the points in the k-nearest set of point x_i * sum of the reach distance of all points in the same set. On the other hand, reach distance is maximum of the

[29] Markus M. Breunig "LOF: Identifying Density-Based Local Outliers" 2000.

[30] Federico Giannoni "Anomaly detection models for IoT time series data" 2018.

[31] Zsigmond Benkő "Model-free detection of unique events in time series" 2022.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

distance of two points and the k-distance of the second points where k-distance is just the distance of a point to the its k-th neighbor.

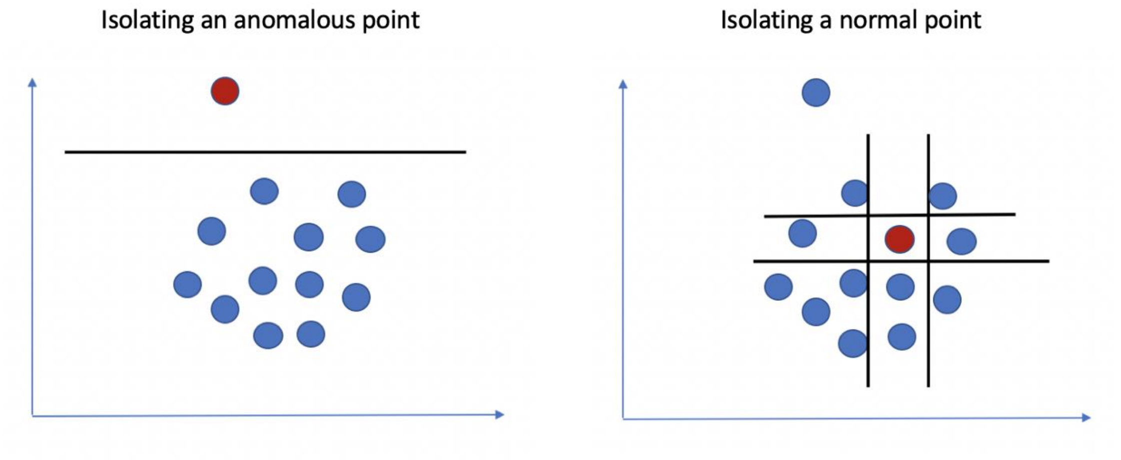
Pros and Cons:

- LOF algorithm can identify outliers in the dataset that would not be outliers in another area of the dataset(Local Anomalies)
- LOF algorithm can even detect outliers that have small distances from their neighbors in dense data clusters.
- As the algorithm gives a ratio(Local Outlier Factor Score), sometimes it is tough to interpret this ratio. There is no specific threshold value above which a point is defined as an outlier. Identification of an outlier is dependent on the problem and the user.

2.2.3.3 Isolation Forest

Most existing model-based approaches to anomaly detection construct a profile of normal instances, then try to capture instances that do not conform to the normal profile as anomalies. Isolation Forest algorithm is a totally different model-based method that explicitly isolates anomalies.[32] The isolation Forest algorithm takes advantage of two properties of anomalies. First is that anomalies are the minority consisting of fewer instances. Second, the values of their attributes are far different from those of normal instances. The term isolation means separating an instance from the rest of the instances. Since anomalies are few and different and therefore they are more susceptible to isolation. In the definition of the algorithm, the separation of instances is repeated until all instances are isolated. This partitioning procedure produces shorter paths to the root node in the constructed tree for anomalies since fewer instances of anomalies result in a smaller number of partitions and instances with distinguishable feature values are more likely to be separated in the early phase of the partitioning procedure.

[32] Fei Tony Liu , Zhi-Hua Zhou “Isolation Forest” 2008.



Isolating an anomalous point

Isolating a normal point

Figure 2.2: The Structure of Isolation Forest

In [33] Isolation Forest is utilized to capture anomalies in the time series dataset. IForest shows superior performance compared to many other unsupervised anomaly detection algorithms. Its cost-optimized nature with good detection performance is the most desirable property of the algorithm.

Algorithm:

1. Randomly select feature q and split value p.
2. Divide dataset X into two subsets by using split value p. These subsets will correspond to a left subtree and a right subtree.
3. Repeat steps 1-2 recursively until the current node has only one sample.

Anomaly Score for Isolation Forest:

$$s(x,m) = 2^{\left\{\frac{-E(h(x))}{c(m)}\right\}}$$

$-E\big(h(x)\big)$ is equal to the average path length of the selected point x in all iTree collections. $c(m)$ Is equal to the average path length of all points in $\{x_1, x_2, \dots, x_m\}$ in all ith tree collections.

[33] Yu Qin , YuanSheng Lou "Hydrological Time Series Anomaly Pattern Detection based on Isolation Forest" 2019; Julien Audibert "Unsupervised Anomaly Detection in Time-Series" 2021; Matteo Paltenghi "Time Series Anomaly Detection for CERN Large-Scale Computing Infrastructure" 2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Interpretation of Anomaly Score:

If $s(x, m)$ returns very close to 1, then those points are more likely to be anomalies.

If $s(x, m)$ returns much smaller than 0.5 then they should be interpreted as normal.

If $s(x, m)$ returns around 0.5 then the entire dataset does not contain any distinct anomaly instance.

Pros and Cons:

- Compared to specially density-based methods, isolation forest is significantly faster.
- Forest gives very good accuracy with small sample size.
- It can scale up large dataset with high dimensions and large number of irrelevant features.
- When dataset is large, performance of the algorithm can underperform due to masking effect that may occur in the dataset.

2.3 Conclusion

In conclusion, time series anomaly detection is the process of identifying anomalies in time series datasets. There are various techniques for anomaly detection, including supervised, unsupervised, and semi-supervised methods. These techniques can be further divided into statistical and machine learning-based approaches. Statistical methods include hypothesis testing, SVD and ARIMA models, Holt-Winters, Wavelet analysis, Fourier Transform, and extreme value theory. Machine learning-based methods include clustering methods, Bayesian models, support vector machines, K-Nearest Neighbors, and tree-based models. In this project, we aim to use autoencoders and deep ensemble autoencoders as base models for anomaly detection. These models have been shown to be effective in identifying outliers in a dataset by comparing their ability to regenerate original data versus anomalous data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 References

[1] https://landing.ai/data-centric-ai/

[2] https://datacentricai.org/

[3] Isabelle Guyon, Nada Matic, Vladimir Vapnik, et al. Discovering informative patterns and data cleaning., 1996.

[4] Tommasi, T., Patricia, N., Caputo, B., & Tuytelaars, T. (2017). A deeper look at dataset bias. In Domain adaptation in computer vision applications (pp. 37-55). Springer, Cham.

[5] Abedjan, Z., Chu, X., Deng, D., Fernandez, R.C., Ilyas, I.F., Ouzzani, M., Papotti, P., Stonebraker, M., Tang, N.: Detecting data errors: Where are we and what needs to be done? Proc. VLDB Endow. 9(12), 993–1004 (Aug 2016). https://doi.org/10.14778/2994509.2994518

[6] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.

[7] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58

[8] Spence, C., Parra, L., and Sajda, P. 2001. Detection, synthesis and compression in mammographic image analysis with a hierarchical image probability model. In Proceedings of the IEEE Workshop on Mathematical Methods in Biomedical Image Analysis. IEEE Computer Society, 3

[9] Aleskerov, E., Freisleben, B., and Rao, B. 1997. Cardwatch: A neural network based database mining system for credit card fraud detection. In Proceedings of the IEEE Conference on Computational Intelligence for Financial Engineering. 220—226

[10] Fujimaki, R., Yairi, T., and Machida, K. 2005. An approach to spacecraft anomaly detection problem using kernel feature space. In Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. ACM Press, 401--410.

[11] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.

[12] H. -S. Wu, "A survey of research on anomaly detection for time series," 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2016, pp. 426-431, doi: 10.1109/ICCWAMTIP.2016.8079887.

[13] 1 Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., & Zhang, Q. (2019, July). Time-series anomaly detection service at microsoft. In Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining (pp. 3009-3017).

[14] 1 Chandola. V, Banerjee. A, Kumar. V, "Anomaly Detection: A Survey", ACM Computing Surveys, Vol.41, No.3, pp. 1-58, Nov, 2009

[15] 1 Percentage points for a generalized ESD many-outlier procedure. Technometrics 25, 2 (1983), 165–172.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[16] 1 Ajay Mahimkar, Zihui Ge, Jia Wang, Jennifer Yates, Yin Zhang, Joanne Emmons, Brian Huntley, and Mark Stockert. 2011. Rapid detection of maintenance induced changes in service performance. In Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies. ACM, 13.

[17] 1 Holt-Winters forecasting Procedure. Journal of the Royal Statistical Society, Applied Statistics 27, 3 (1978)

[18] 1 Wei Lu and Ali A Ghorbani. 2009. Network anomaly detection based on wavelet analysis. EURASIP Journal on Advances in Signal Processing 2009 (2009), 4.

[19] 1 Faraz Rasheed, Peter Peng, Reda Alhajj, and Jon Rokne. 2009. Fourier transform based spatial outlier mining. In International Conference on Intelligent Data Engineering and Automated Learning. Springer, 317–324.

[20] 1 Alban Siffer, Pierre-Alain Fouque, Alexandre Termier, and Christine Largouet. 2017. Anomaly detection in streams with extreme value theory. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 1067–1075.

[21] 1 LI,H 2010.Research and Implementation of an Anomaly Detection Model Based on Clustering Analysis. International Symposium on Intelligent Information Processing and Trusted Computing

[22] 1Moore, D.2005. Internet Traffic Classification Using Bayesian Analysis Techniques. in Proceedings of ACM SIGMETRICS.; Johansen, K. and Lee. ” CS424 network security: Bayesian Network Intrusion Detection (BINDS)”: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1 .83.8479

[23] 1 Mukkamala,S.,Sung, A.and Ribeiro, B.2005. Model Selection for Kernel Based Intrusion Detection Systems. Proceedings of International Conference on Adaptive and Natural Computing Algorithm.

[24] 1 Ming, Y. 2011. Real Time Anomaly Detection Systems for Denial of Service Attacks by Weighted k-NearestNeighbor Classifiers”. Expert Systems with Applications, Vol.38, 2011, pp. 3492-3498.

[25] 1 Peddabachigari, S., Abraham, A., Grosan, C. and Thomas, J. 2007.” Modeling Intrusion Detection System using Hybrid Intelligent Systems”. J. Netw. Comput. Appl, Vol. 30, NO1, PP. 114-132.

[26] 1 Sangmin Lee, Hak Gu Kim, and Yong Man Ro. Stan: Spatio-temporal adversarial networks for abnormal event detection. arXiv preprint arXiv:1804.08381, 2018.

[27] 1 MATE SZEKER. Spatio-temporal outlier detection in streaming trajectory data, 2014.

[28] 1 Donghwoon Kwon, Kathiravan Natarajan, Sang C Suh, Hyunjoo Kim, and Jinoh Kim. An empirical study on network anomaly detection using convolutional neural networks. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pages 1595–1598. IEEE, 2018.

[29] 1 Markus M. Breunig “LOF: Identifying Density-Based Local Outliers” 2000.

[30] 1 Federico Giannoni “Anomaly detection models for IoT time series data” 2018.

[31] 1 Zsigmond Benkő “Model-free detection of unique events in time series” 2022.

[32] 1 Fei Tony Liu , Zhi-Hua Zhou “Isolation Forest” 2008.1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[33] Yu Qin , YuanSheng Lou “Hydrological Time Series Anomaly Pattern Detection based on Isolation Forest” 2019; Julien Audibert “Unsupervised Anomaly Detection in Time-Series” 2021; Matteo Paltenghi “Time Series Anomaly Detection for CERN Large-Scale Computing Infrastructure” 2020

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739