DASMA : Towards Real-time and Explainable Anomaly Detection on Data Stream

Florentin Jiechieu

PhD, PostDoc, CNRS-LIMOS

florentin.jiechieu_kameni@uca.fr

Plan

- Context and Objectives
- Anomaly Detection Algorithms on Data Stream
- Explainability Methods
- System Validation
- Future Directions

Section 1

CONTEXT AND OBJECTIVE

DASMA PROJECT

DASMA is a 3-year research project started in 2021 and funded by BpiFrance and led by Pr. **Engelbert MEPHU NGUIFO**.

Overall objective :

Build a monitoring system that will help users to efficiently analyze data streams and identify potential anomalies in real-time.

Context

- A data stream refers to an infinite volume of data that arrives continuously
- Data streams appear in many context : from monitoring systems based on sensors to social media including financial transactions.
- Anomaly detection is a topical issue when analyzing data from a datastream.

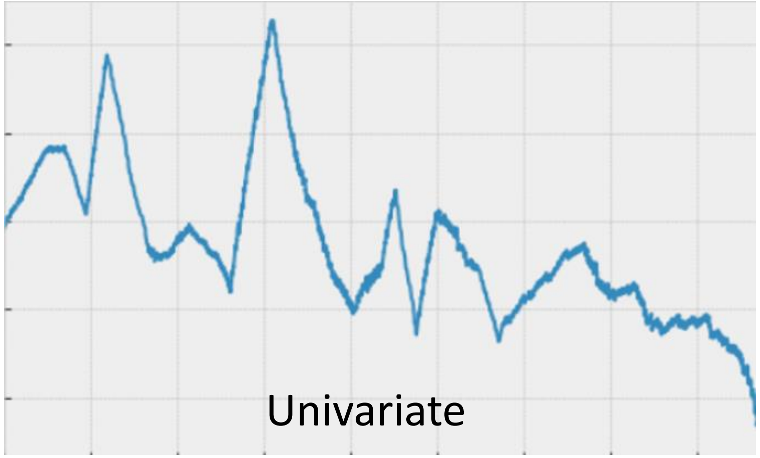
Fig. 1: Monitoring farm

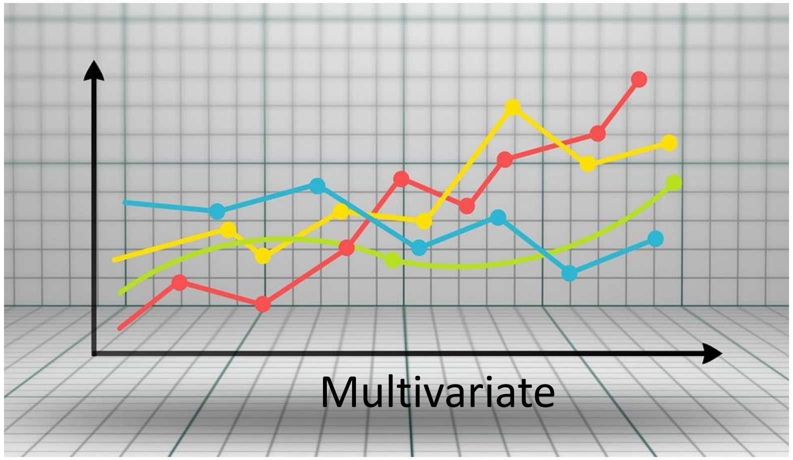
Fig. 2: Financial transanctions

Fig. 3: Monitoring white rooms

Data stream and Multivariate time series

- Time series analysis refers to the study and analysis of sequence of time-ordered data points.
- Depending on the number of variables or series being studied we distinguish univariate and multivariate time series
- A data stream consisting of numerical and multivariate data points can be seen as an infinite multivariate time series.





Types of anomalies in time series

Anomaly detection refers to the identification of rare events that differ significantly from the normal trend observed in the data distribution

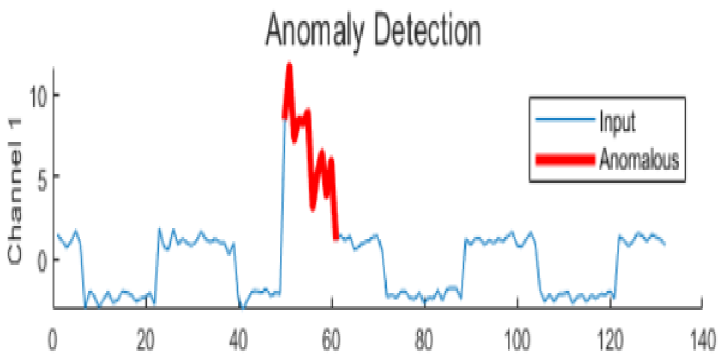


Fig. 4: Collective anomaly

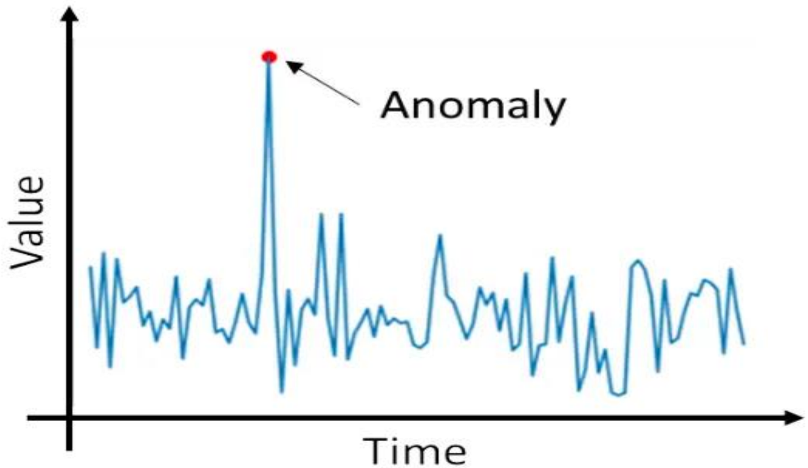


Fig. 5: Point Anomaly

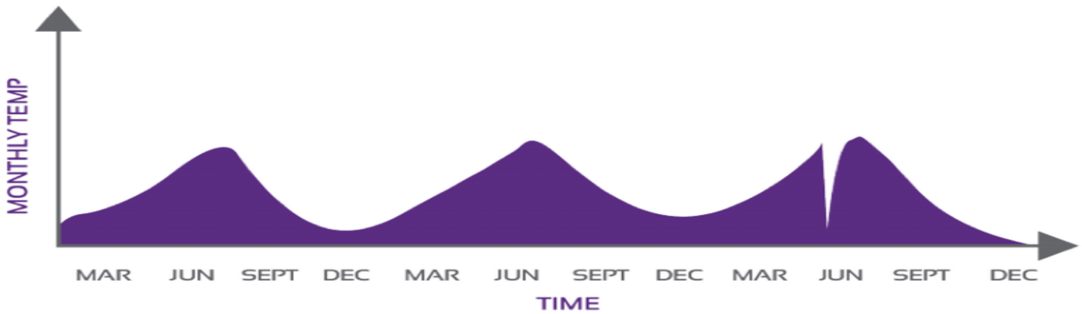


Fig. 6: Contextual anomaly

Objective et Challenges

Main objective: Built a real-time anomaly detection system on data streams that is capable of providing real-time explanations to anomalies detected

Challenges :

- **Data:** High volume of data, infinite, dimensionality of data, normalizing data.
- **Analysis:** Accuracy, Real-time, Explainability, domain knowledge.
- **Unsupervised:** Unlabelled data, Unknown parterns

Section 3

ANOMALY DETECTION METHODS

Classification of anomaly detection methods for data stream

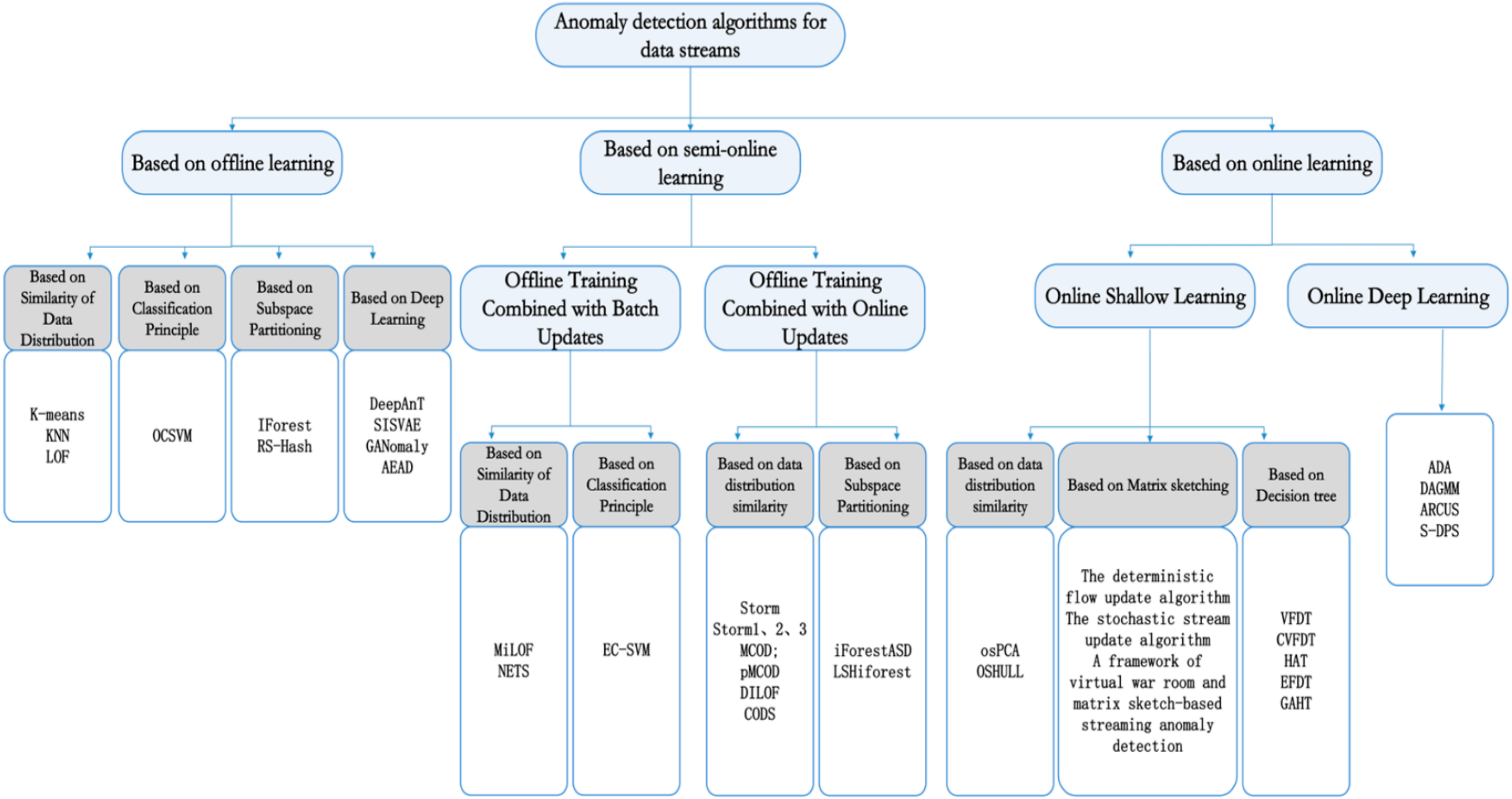
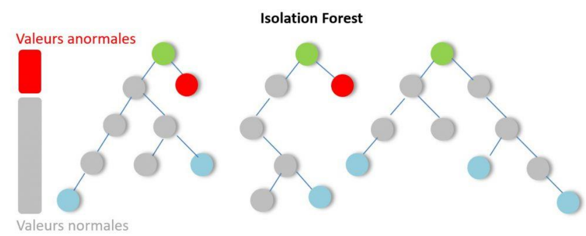
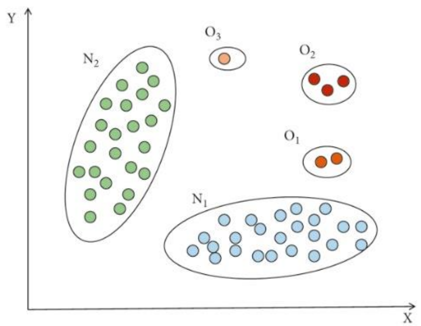


Fig. 8 : Tianyuan Lu, Applied Science 2023

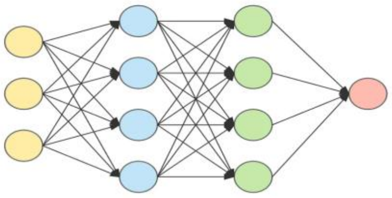
Methods studied yet

Methods based on subspace partitioning





Methods based on clustering



Methods based on deep learning

Ensemble Methods

Deep learning based methods

AUTOENCODER

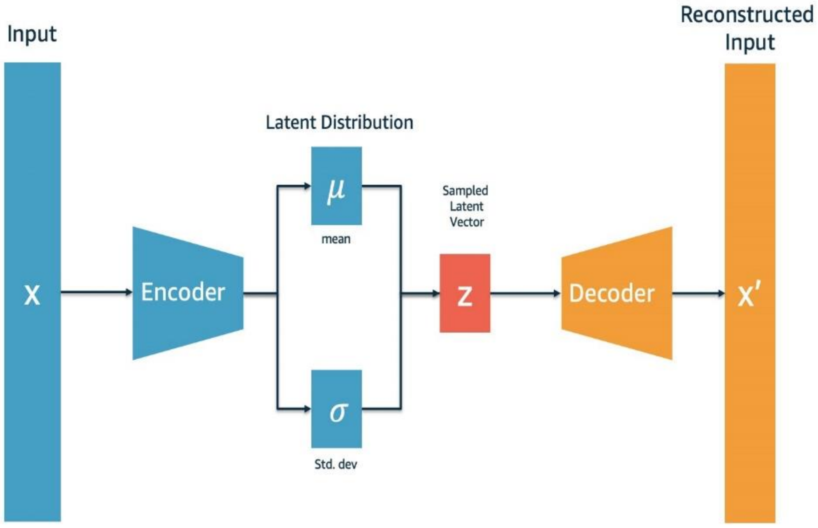


Fig. 9: Yi Xiang, Amazon MSL, 2021

GAN

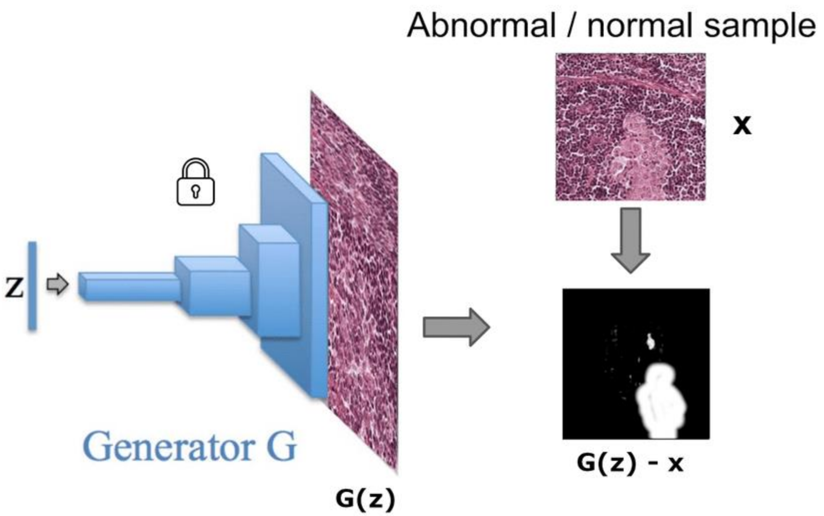


Fig. 10: Dejan Stepec et al., MICCAI 2020

DEEPANT

- **Principle :** Leverage on convolutional neural networks to predict a data point of the datastream based on a subsequence of the datastream.

- A windowing technique is used to update the model periodically

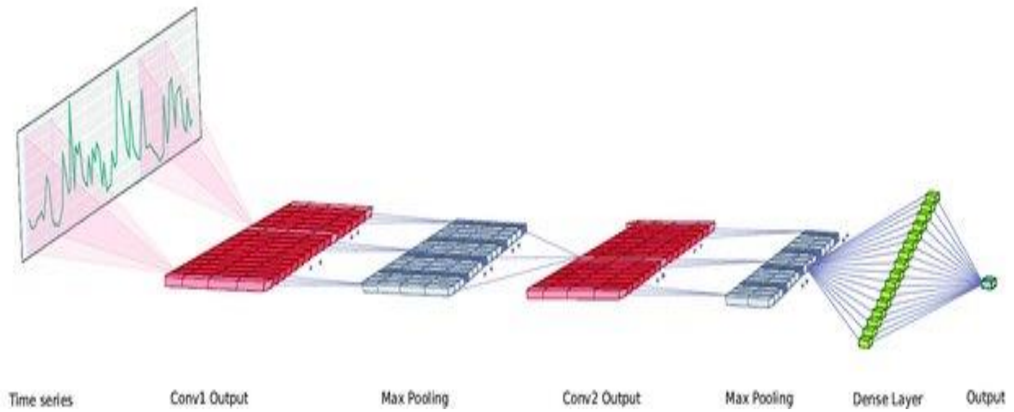
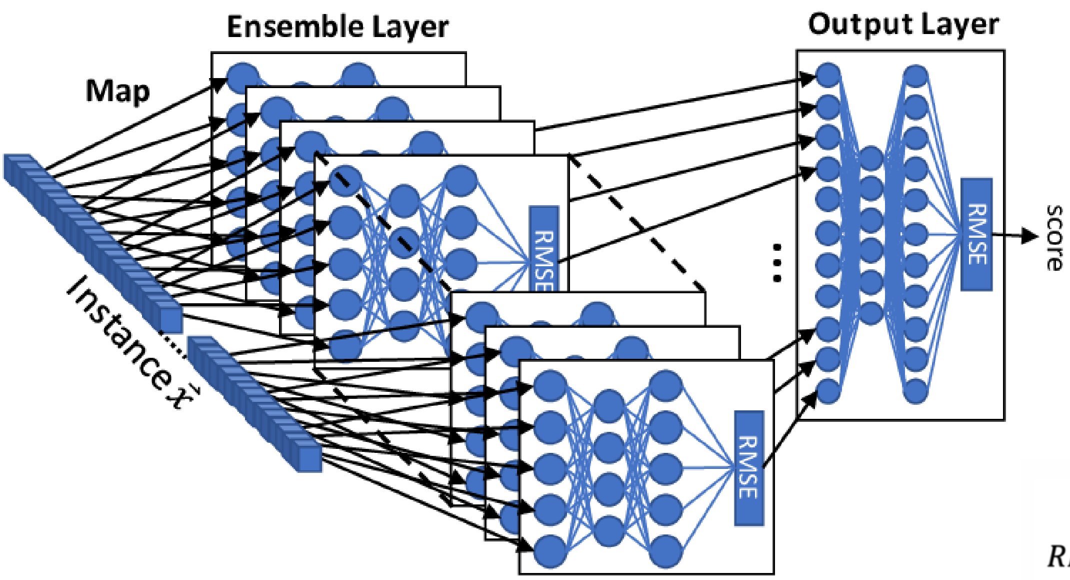


Fig. 11: Yi Xiang, Amazon MSL, 2021

KitNet Anomaly Detection Algorithm

- **Principle :** KitNet is an online and unsupervised anomaly detection algorithm based on autoencoder. KitNet was originally designed to detect network intrusions.

- RMSE = Root Mean Square Error



$$RMSE = \sqrt{\frac{\sum_{i=1}^{N} \|y(i) - \hat{y}(i)\|^2}{N}},$$

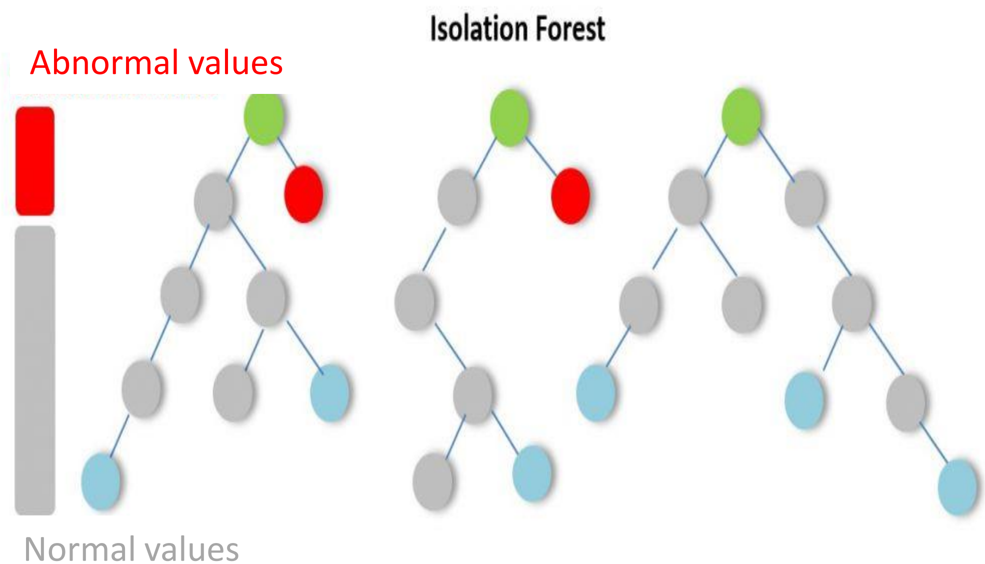
Fig. 12: Yisroel, NDSS, 2024

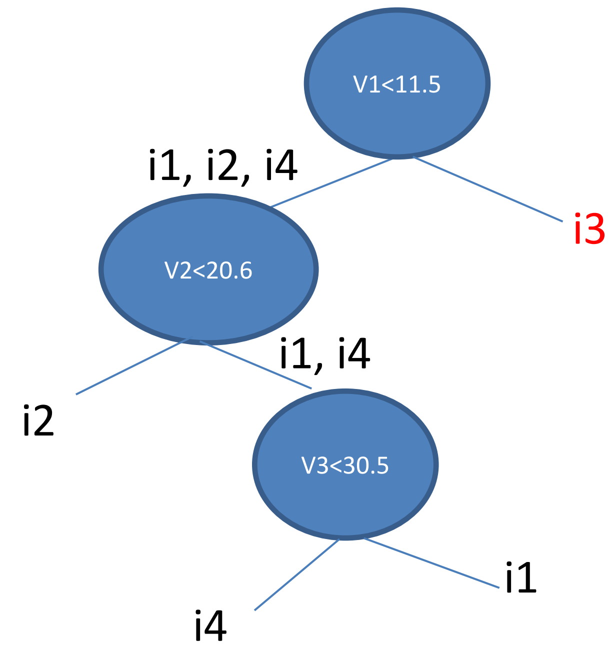
Isolation forest principle

Principle : 1. Build an isolation forest where each subtree represents a subpartition of the original data based on the value of a dimensional variable.

2. Classify each point in the trees following the nodes conditions. If the point is isolated very early, then it might be an anomaly.

	v1	v2	v3
i1	11	21	31
i2	10	20	33
i3	15	25	33
i4	10	21	





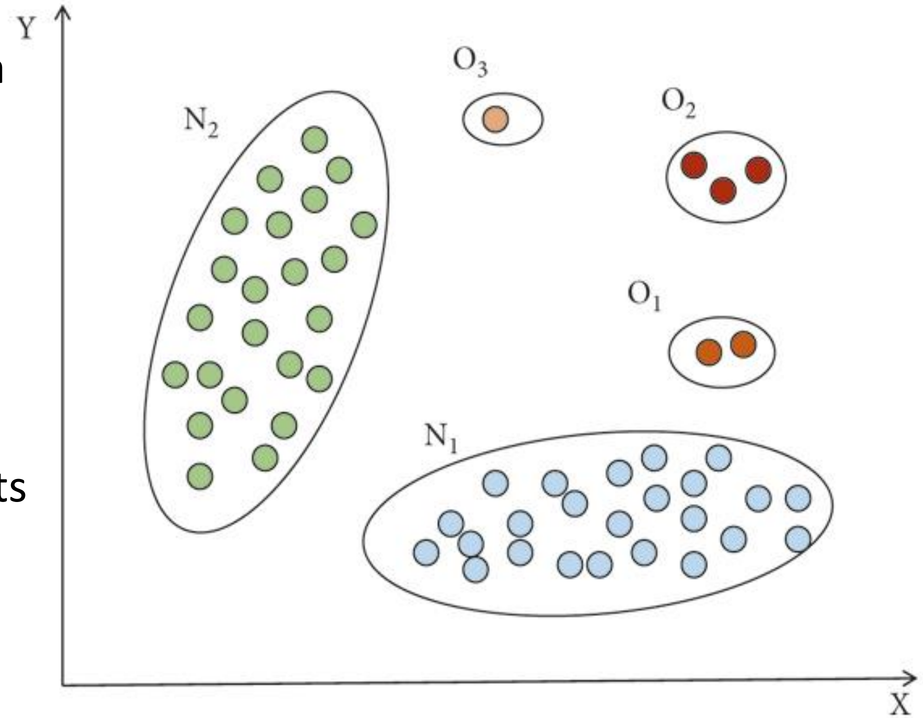
HSTREE & IFOREST

Clustering (Distance/Density)

- **Principle :** Identify data clusters using a clustering. The data that are isolated from clusters are considered abnormal.

In this category we have:
LOF, MILOF and **DRAGSTREAM**

In the context of a datastream : Data points are theoretically infinite.



Ensemble methods

Principle : use multiple anomaly detection methods and agregate the results

Challenge : Normalize the ouput of the various methods

Real –time : Synchronize all the anomaly detectors. Issue with the real-time constraint

Interpretability ?

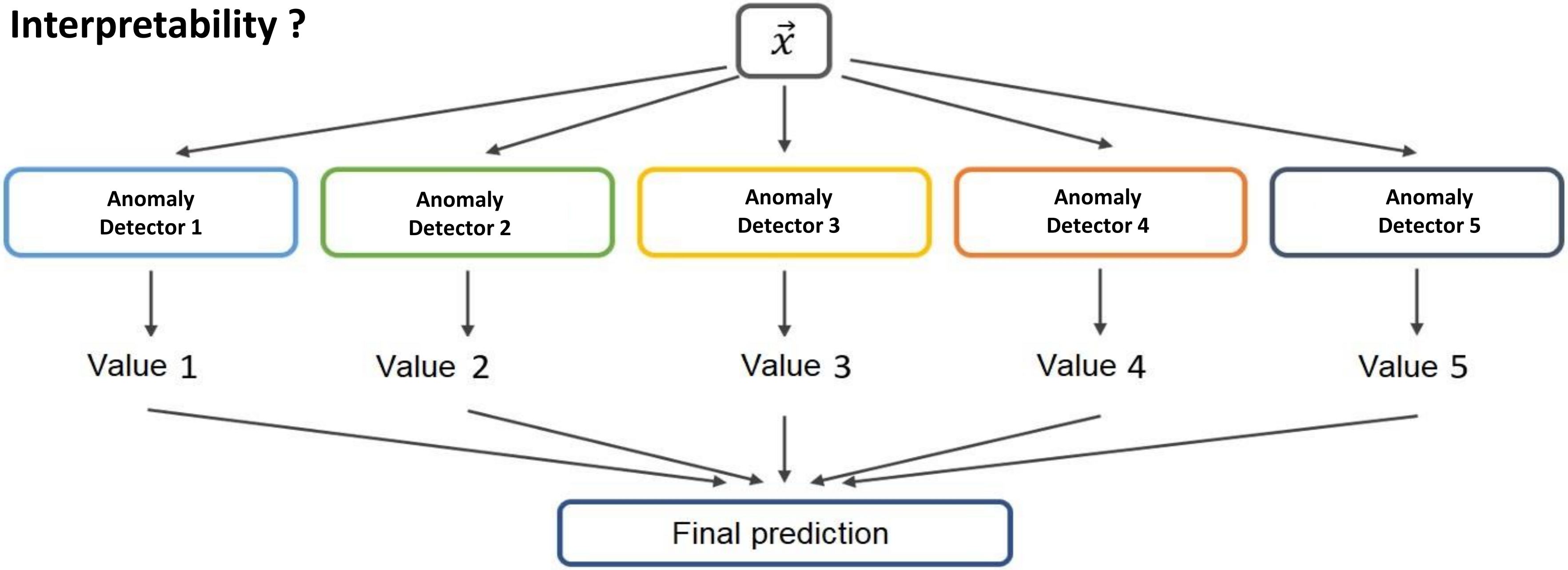


Fig. 13: Ensemble methods

How do we process the datastream ?

A datastream is theoretically infinite

The windowing technique is used to determine which part of the stream is used to update the model.

- Landmark window (i)
- Sliding window (ii)
- Damped window (iii)

Drawback (i & ii): difficult to determine the size of the window . Points in the window are consider of equal importance.

Drawback (iii) : interpretability, Time complexity.

Other : Incremental learning

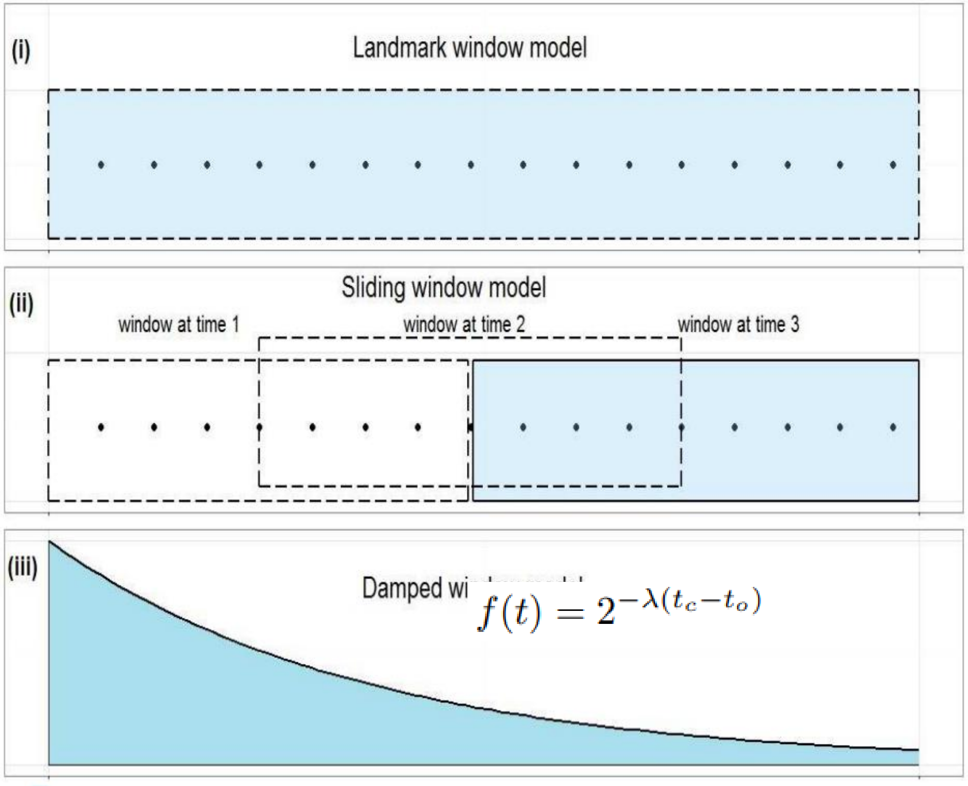


Fig 14. Windowing (S. Mansalis et al, 2018)

Section 3

EXPLAINABILITY

Why explaining?

Objective: Identify uncommon behavior in the distribution of the datastream

Measures	v1	v2	v3	v4	Anomaly score
M1	2.60	0.054	0.148	0.003	0.2
M2	2.51	0.055	0.155	0.005	0.41
M3	2.52	0.2	0.206	0.001	0.9
⋮	⋮	⋮	⋮	⋮	⋮
M10	2.53	0.3	0.139	0.004	0.95
	⋮	⋮	⋮	⋮	⋮

- Why anomaly detected on M3 and M10 ?
- Should we fire an alert ?

Fig. 14: Why explaining ?

Score attribution local explainability

- Objective : assign a score representing the contribution of each variable to the value predicted.

The greater the score
The more important is
the feature.

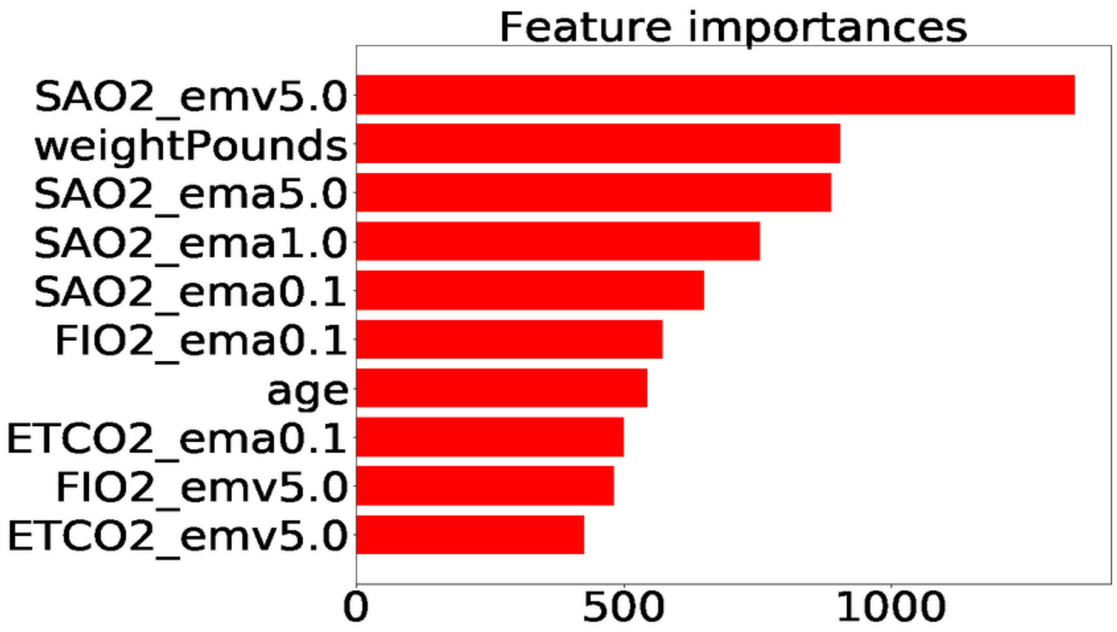


Fig. feature importance.

LIME & SHAP

- Both are model agnostic
- They both perform local explanation

- **LIME :** find a simple and explainable model that maximizes the faithfullness with the prediction of the real model in the neighborhood of the instance to explain

- **SHAP :** Assign to each feature a score representing the importance of including that feature in the input.

$$Explanation \quad = \sum_{k=1}^{n} \alpha_i X_i$$

Avantage : Genericity

drawback : slow

LIME (Ribeiro et al., 2016)

Objective : Find a model locally interpretable that best approximate the behavior of the original Model in the neighborhood of the instance to explain.

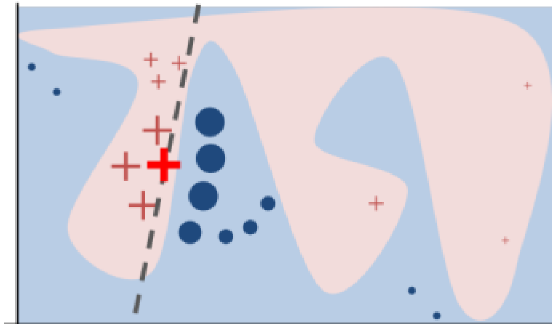
Explainable function that locally approximate *f*

$$\xi(x) = \operatorname*{argmin}_{g \in G} \; \mathcal{L}(f, g, \pi_x) + \Omega(g)$$

Measures the non fidelity of *g* with respect to f

Measure the locality to *x*

Complexity of *g*



The more the model is complex, the less it is interpretable

Advantage : Genericity

Drawback : Slow

SHAP

Objective : Assign an importance to each feature that represents the effect of including that feature on the output produced by the model.

Model including feature *i*

$$\phi_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|!(|F| - |S| - 1)!}{|F|!} \left[f_{S \cup \{i\}}(x_{S \cup \{i\}}) - f_S(x_S) \right].$$

Model without *i*

Importance of the feautre *i*

Mean

Importance of including *i*

(M. Lundberg et al., NeuRIPS 2017)

The more complex is the model, the less it is interpretable

Advantage : Genericity

Drawback : Slow

Section 4

VALIDATION

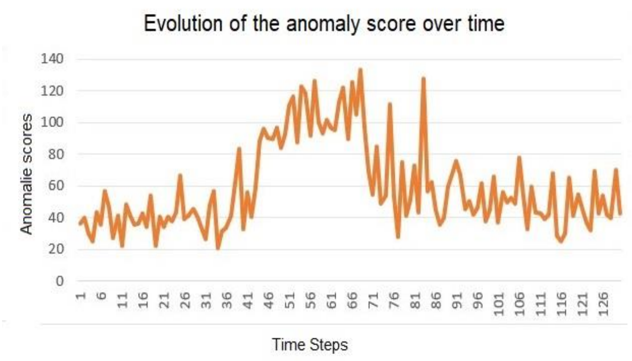
SYSTEM CONFIGURATION

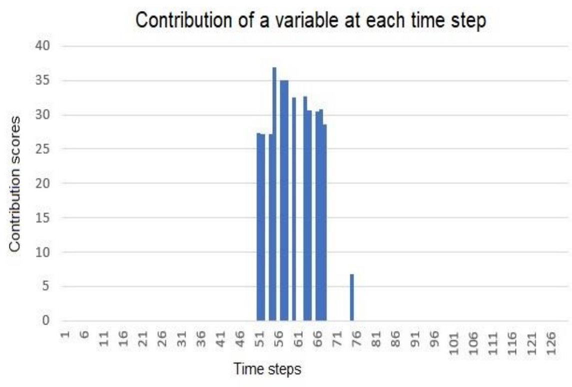
1. Simulate a data stream from CSV files

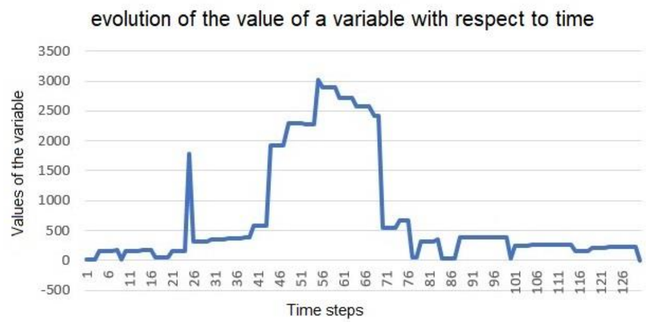
2. Report the points where the anomaly score are greater than the specified threshold

3. Report the contributions of the various variables

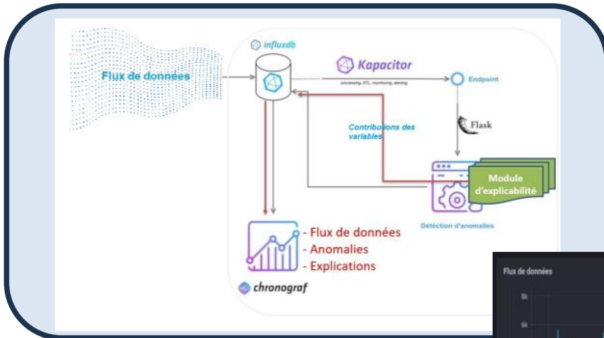
4. Expert validation : Monitor the variables with the highest contributions and check if there was something abnormal with them during the time that the anomaly score was greater than the threshold





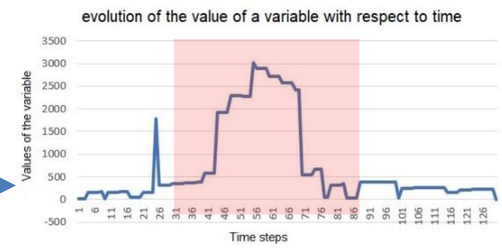


THE SYSTEM AT A GLANCE



System architecture

3 Observe the trend of those variables

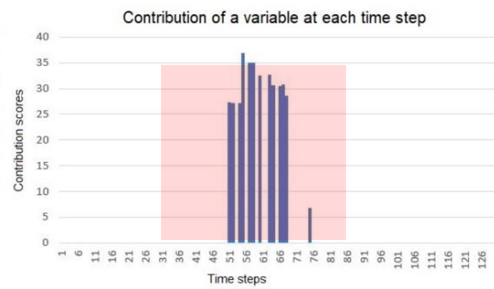


DASHBOARD

2 Identify the most contributing variables

1 Monitor anomaly scores

Identify and understand anomaly detected thanks the triad : anomaly score, contributions and the stream.



Architecture

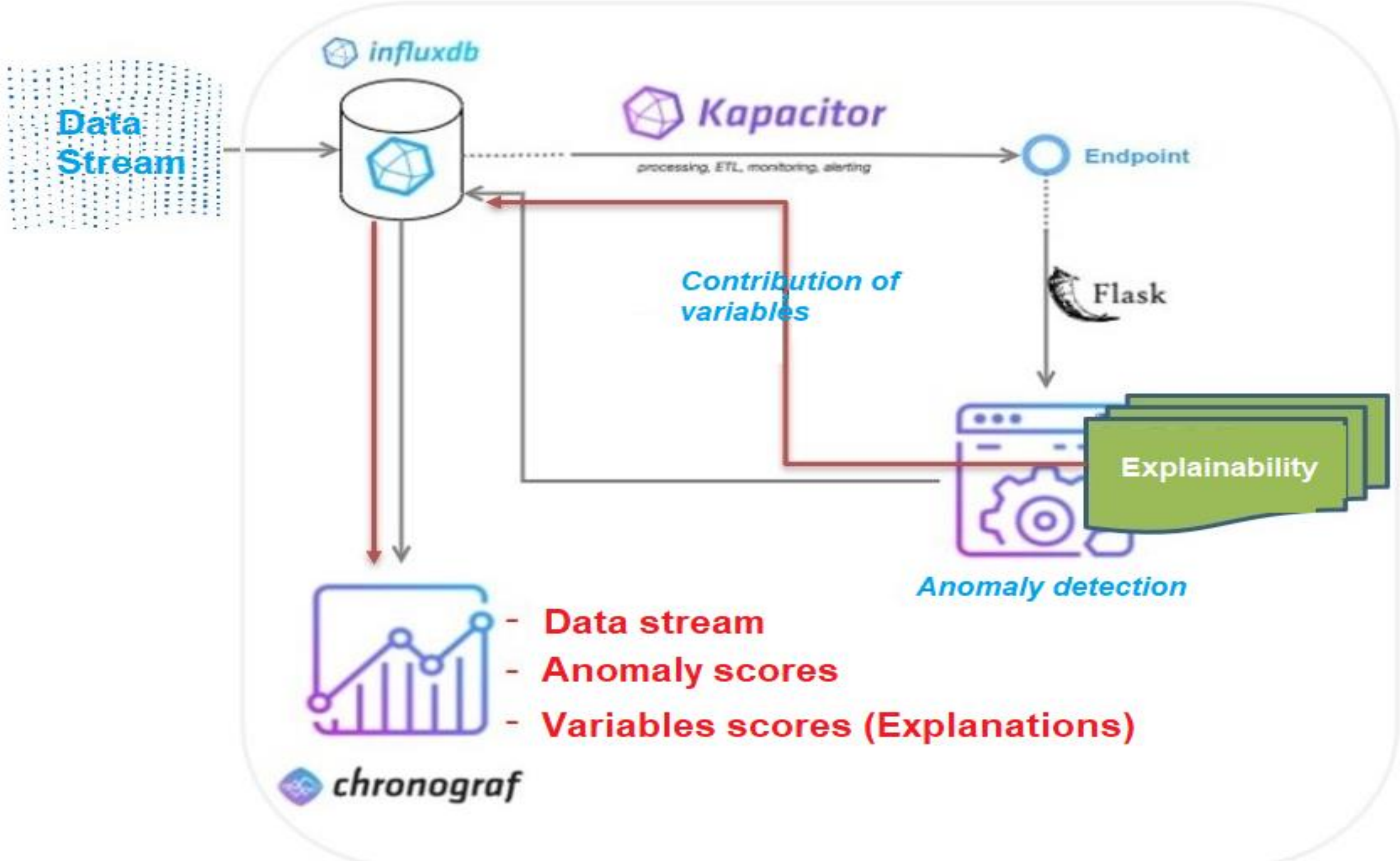


Fig. 7: System architecture

Section 5

FUTURE WORKS

In progress

- Explainability: quality and real-time
- Anomaly detection : quality and real-time
- Multivariate analysis vs univariate analysis
- Effective continuous learning
- Effectively handle the concept drift
- Fixed threshold vs dynamic threshold
- Graphic User Interface

PUBLICATIONS

- Jiechieu Kameni Florentin Flambeau, Anne Marthe Sophie Ngo Bibinbe, Vasilis Cako, Abdoul Jalil Djiberou Mahamadou, Mohamed Rayane Bakari, Kevin Dilan Nguetche, Durande Kamga Nguifo, Anthony Bertrand, Michael Franklin Mbouopda, Rim El Cheikh, Gertrude Raissa Mbiadou Saleu and Engelbert Mephu Nguifo : **SEDAF : Prototype d'un Système Explicable de Détection d'Anomalies dans les Flux de Données,** EGC 2024: xxx-xxx, Dijon, Janvier. RNTI

- A. M. S. N. Bibinbe, A. J. Mahamadou, M. F. Mbouopda and E. M. Nguifo, "DragStream: An Anomaly And Concept Drift Detector In Univariate Data Streams," *2022 IEEE International Conference on Data Mining Workshops (ICDMW)*, Orlando, FL, USA, 2022, pp. 842-851, doi: 10.1109/ICDMW58026.2022.00113.

- Anne Marthe Sophie Ngo Bibinbe, Michael Franklin Mbouopda, Gertrude Raissa Mbiadou Saleu, Engelbert Mephu Nguifo: Évaluation comparative de méthodes non supervisées pour la détection de points anormaux dans les flux de données. EGC 2022: 493-494

- Anne Marthe Sophie Ngo Bibinbe, Michael Franklin Mbouopda, Gertrude Raissa Mbiadou Saleu, Engelbert Mephu Nguifo: A survey on unsupervised learning algorithms for detecting abnormal points in streaming data. IJCNN 2022: 1-8

Thank you for your kind attention
!