A New Centralized Detection-Based Process for Evaluating Anomalies and Analyzing the First Causes Using Machine Learning and Web Semantic

https://doi.org/10.3991/ijoe.v19i03.30079

Abdellatif Lasbahani[1(✉)], Rachid Tahri[2], Abdessamed Jarrar[3], Youssef Balouki[2]
[1]Laboratory EMI, University Sultan Moulay Slimane, Beni Mellal, Morocco
[2]Faculty of Sciences and Techniques, Hassan First University, Settat, Morocco
[3]Faculty of Sciences, Mohammed First University, Oujda, Morocco
abbdellatif.lasbahani@gmail.com

Abstract—In the last decades, many works have been done to enhance data performances in the computer field. Data performance consists to describe all improvements which can be added to data traffic. More precisely, we are talking about techniques allowing improving the evaluation of big data using machine learning. Data evaluation is composed of several variables such as security, quality of service, data synchronization, scalability, and data structuring. In this work, we complete our proceedings done to supervise the continuity of technological evolution in terms of big data and safety. In other words, we aim to add brick to our previous processes to take into consideration the enhancement of the analysis of the causes generating frauds and intrusions preventing data traffic. To achieve this end, we increase current machine learning techniques with prior knowledge based on data thresholds set by experts in the first place. We also aim to integrate knowledge facilitating the interpretation of the causes causing all kinds of anomalies in the second place. Finally, our process will be endowed with the requirements to improve the rate of detection of anomalies and reduce human involvement operation.

Keywords—anomaly detection, semantic web, knowledge graphs, machine learning, frauds and intrusions, prior knowledge, data thresholds, deep cause's analysis

1 Introduction

Recently, we have assisted a technological growth in several topics. As an example, we focus on the field of the Internet of Things (IoT), which has seen an emergence and technological remarkable migration. These IoTs components constantly create and generate data which focuses on the description of the statue, the environment and the context of this data. For this purpose, there are a variety of components integrating the principle and logic of the Internet of Things such as sensors. Sensors monitoring systems have deployed into almost industries, a variety of research domain and applications as healthcare and logistics. Such technology can give useful information's

into an institution's physical objects and the connection and interaction between these objects. However, awareness in the industrial environment has become an obligation requiring placing and implementing more intelligent objects or sensors integrating data analysis. Data-driven investing provides a valuable position for companies that have this advantage. From a safety point of view, there are two more gifted methods; we find the Anomalies Detection (AD) and Deep Causes Analysis (DCA), which ensure the irregular investigation of the data. Indeed, these methods and tools are becoming more accessible and available in order to add more considerations to the data in the analysis phase and even implementation in the field of exploitation.

Anomalies Detection is a step in data mining process which consists of identifying data points, events, and / or observations that deviate from a dataset's normal behavior. In other words, this processus can indicate critical incidents distributed over several types such as a technical glitch, or potential opportunities, for instance a change in consumer behavior, also identifying behaviors that do not match design patterns and other elements within a data set [1]. while, DCA aims to lead the error correction process by teaching resolvers to the main real causes of the detected anomaly [2].

In Figure 1, we represent our anomaly detection process proposed during our work [3]. In this process, we focus on the usual workflow. First, the data coming from several sources will be considered as pre-requisites necessary to accomplish the pre-processing phase whose goal is to ensure the uniformity of the data. Thus, the cleaning phase will be considered a preliminary phase that precedes the learning phase of our model according to regular expressions and logical restrictions in order to detect the rules of associations and the famous characteristics. Subsequently, these models and expressions will be used to upgrade the data by detecting anomalies occurring on the new data. However, the divergence between the learned model and the new data gives rise to a foreign anomaly, and thus an adapted action and mechanisms will be proposed according to the deep analysis of the main causes behind this divergence or unusual behaviour. Therefore, a more relevant solution will be proposed to resolve the main causes alongside this divergence.

More concretely, we take as an example the forest fire prediction system. Historical sensor data will be used to anticipate the average heat or temperature level (C) the new sensor data will be used to ensure areas whose temperature diverges from the learning patterns. Indeed, monitoring and intervention systems will be triggered.

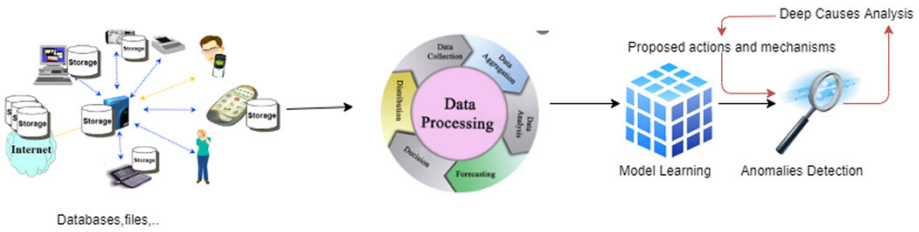

Fig. 1. Anomalies detection process

According to our study and in-depth research done in this direction, the AD and DCA tools previously proposed suffer from the lack of measurement of the evolution and changes of possible behaviours in various contexts. Considerations related to the

external environment can be one of the reasons causing the temperature variation whose prediction system considered them how abnormal behaviours. Consequently, he will be unable to react because his learning model has not yet had such unusual data. In fact, human intervention is needed to familiarize this system with several considerations related to the environment, climate change and variation in coordinates. Specifically, discarded sensors can proportionally produce data quickly. While a regular analysis will be essential to have observations on abnormal behaviours on the one hand, and to monitor the flows being activated on the other hand. However, this dataset requires more precision which leads to a lot of false alerts and undetected behaviours [4].

Therefore, an upgrade for anomaly detection tools in contextual environments should be prioritized, with the aim of strengthening current systems to take more advantage of technological growth in terms of data. In our example, multi-variable climate change could be used as prior knowledge to strengthen and optimize the forest fire safety process.

In summary, the main objective and challenge of this work is to make stronger our process of detecting anomalies and automatically extracting knowledge [3] of new mechanisms and strategies more detailed in the following points:

1. Reduce the number of frauds and anomalies generated immediately based on the knowledge deduced from a structured dataset.
2. Reduce the gap in frauds and anomalies falsely generated based on prior knowledge.
3. Enrich the process of detecting and correcting [3] the potential for variation in contextual environments.
4. Automate the detection of major causes causing such anomalies.
5. Automate the interpretation of the main causes of anomalies in order to frame them and allow the automatic generation of appropriate mechanisms and solutions by integrating context-related data.
6. Generalize the detection behaviour according to changes in measures related to the environment and the context of use by reducing the involvement of specialists and humans during the design of this divergence.
7. Adopt the detection learning model to integrate possible changes related to desirable behaviours in a given context.

In the next section, we present an overview of the work carried out in this subject of study. We will focus on approaches and methodologies representing essential axes for our strategic and organizational focus of our targeted process.

2 Related works

In this section let's present the various advanced and more gifted works presented in the field of strengthening the security aspect by drawing more from the technological growth brought with the arrival of machine learning. More precisely, we will focus on approaches based on the knowledge previously available to improve the detection of anomalies and the deep analysis of the causes causing this kind of poorly planned behaviour. In the first place, we present the famous works projectinglearning models that use the available knowledge as input. Secondly, we focus on techniques and tools

that react directly with the contextual environment and its content in terms of available information. Third, we focus on rule-based anomaly detection mechanisms. Finally, we present the intrusion detection systems given up to the moment by visualizing the advantages and disadvantages of each.

in recent years, we have witnessed the publication of enormous works and approaches aimed at proving the technological evolution in terms of improving the aspect of detection of fraud and intrusions occurs in network traffic and in data intended to be mined requiring a higher level of criticality. we start with those that present more relevant approaches to support anomaly detection in an unstructured data set, and that do not require models, evaluation thresholds, predefined strategic rules, prior knowledge, or any kind of overarching logical criteria such as [5][6]. In addition, these works promote a very high level in the measure of security aspects for the developers of software systems. Currently, most of the approaches given in this direction are based on Machine Learning (ML) techniquesand this in order to process big data requiring a higher level of vigilance. Machine learning models can be supervised and unsupervised, and this is strongly related to the nature of the data, is what it is labelled or unlabeled data. Therefore, most AD disadvantages are related to the difficulties of categorizing unsupervised learning due to lack of the unpredictable aspect of data.

The main objective of AD is to design and model the normal behaviour to be highlighted during data traffic. Statistical measures can be designed to ensure the involvement of this behavioural model in the temporary and special disaptasure of anomalies when there is a discrepancy in the projection of the data set [7][8]. Therefore, the anomalies detected are so difficult to interpret and analyze in accordance with the laws and rules imposed by the detection models [9]. DCA techniques are based on detection models inspired ontree structures and logics [10].

Nowadays, knowledge and information are projected and represented as a data structure whose elements are connected and interpretable from which environmental strategies can be generated and applied. Such representation is more generally known as the Semantic Web (SW) [11]. SW promotes the consideration of standardized data formats and exchange prototypes on the web based on the Resource Description Framework (RDF). In this context, knowledge can be represented through semantic terms and concepts in a structured set called ontology. It is used to reason about the objects of the domain concerned. For this purpose, these ontology's are used to annotate the prior data and information in order to store them via node-edge triplesin the form of graphical knowledge [12]. However, this representation of knowledge is insupportable by machine learning. In other words, machine learning does not have enough techniques and methods that allow it to derive more from these graphical representations. Therefore, vector transformation techniques and mechanisms became a mandatory necessity, so popular, favouring distributed integration [13]. According to our extensive research in this domain, there is an almost total absence of such an approach to develop anomaly detection systems based on these concepts. Probably, due to the unsupervised nature of the sources involved in the creation of these anomalies.

From a knowledge-based machine learning perspective, data integration and distribution promotes manageable data transformation in the form of more relevant decisions

and knowledge from which systematic and technological wealth will be created. And this by exploiting a lot of methods and techniques previously conducted by experts in various fields. These techniques and methods ensure learning from knowledge graphs without the loss of values, parameters and information's due to embedding transformation. Among these methods is the Relational Graph Convolutional Network (RGCN), a method more similar to neural networks but operating on graphs, designed primarily to process data with multi-rational characteristics [14]. In addition, other areas of research have been able to overcome the weaknesses brought about by previous research by focusing on the development of descriptions of predicates, exploiting the wealth of data available and those previously examined. As an example, we find the Inductive Logic Programming (ILP) approaches based on logic and statistics. Nevertheless, there are other approaches and combinations based on machine learning techniques and prior knowledge models [15].

Therefore, none of these approaches and techniques provides for consideration of variations in data resources. More precisely, we are talking about sensor flows, environmental data of various contexts, and finally all kinds of variant data during manipulation. This hypothesis is strongly related to the lack of consideration of the evaluation of the prediction which requires more prior knowledge of the data context.

About integrating prior knowledge into policy-based systems, Policy-based detection systems require strong human involvement using the expertise of experts in the fields of anomaly resolution, because these policies are more explainable and adaptable to the current problem. However, the available development languages do not adapt to the evolution and continuous growth of data. In fact, we will need more time in the development process as well as human involvement to accomplish these operations [16]. However, current detection mechanisms that emphasize machine learning focus on non-scalable learning models in order to be sustainable and adapt to possible changes in the context of use.

In the following section, we present our proposed approach in the context of anticipating and solving the following problems:

- ✓ Current detection mechanisms using only the data itself to detect unwanted behaviour and actions.
- ✓ The large number of unwanted alarms and frauds generated disrupt the operation of the learning model, which destabilizes the frequency of accuracy.
- ✓ AD and DCA methods work with unchanged data, making it so difficult to process real-time data such as variable data and streaming contexts.
- ✓ AD and RCA's learning models are trained only once, making it impossible to consider change in the context of use so difficult, such as in streaming environments, sensor data and development in new contexts.
- ✓ The design of the RCA model requires a direct human involvement.
- ✓ Lack of evaluation and interpretation of decisions.
- ✓ The lack of self-adaptation of learning models with the change in settings of the deployment environment.
- ✓ Cover the lack of interoperability and data diversity

3 Proposed approach

As part of acquiring our previously suggested objectives, we have re-established our process with techniques and methods based on machine learning, in order to focus mainly on the following hypotheses deduced after our investigations and evaluations of our process in force to the most gifted research in this field.

- Adapt the learning and reasoning algorithms according to prior knowledge in order to achieve a detection rate exceeding by at least 2% the detection percentage of previously negotiated methods.
- Minimize 90% of unwanted signals and alarms causing malfunction in reasoning and learning models.
- Increase by at least 4% false negatives and false positives by integrating prerequisites and prior knowledge.
- Reduce human involvement by more than 75%, in situations requiring a change of parameter in varying environmental contexts.
- Design a learning model applicable to streaming contexts, without causing a mixture of data.
- Adapt our process to consider fraud detection and causes of errors in real time in different contexts.

To achieve these hypotheses, we were able to think of extending our previously proposed process of emphasizing the ability to develop a system that merges machine learning and semantics. Specifically, we have strengthened our anomaly detection process with a further extension of detection techniques based on AD and DCA. This integration will allow us to focus on detecting and analyzing the causes of fraud related to data inside a stream of data with precision. In other words, we describe the divergence of norms and rights for handling online data from different sources.

The main objective is to enrich our process with the prior knowledge from a data stream whose objective is to design patterns to improve AD and DCA detection techniques with the necessary guidelines and prerequisites. This extension will facilitate fraud detection and also to address the research questions described in the previous section. An overview of this new extension of our process is given in Figure 2.

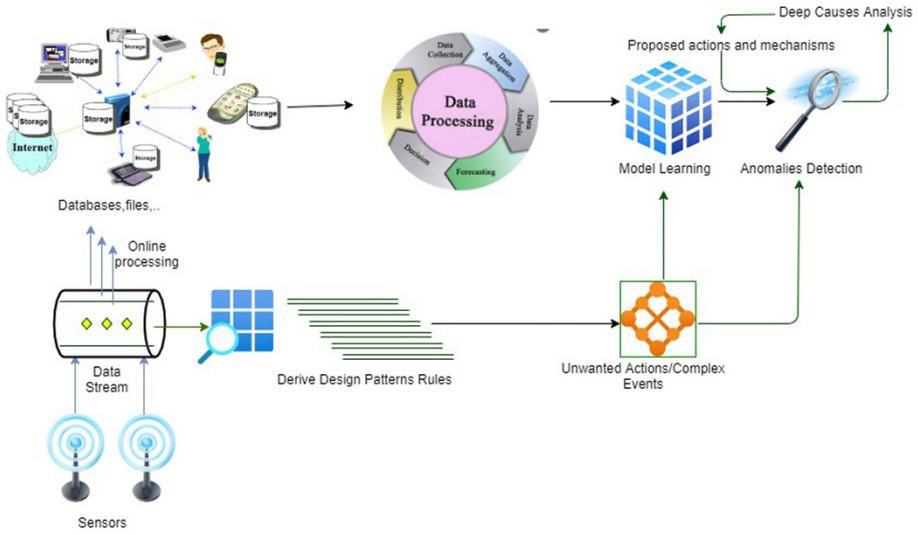

Fig. 2. Overview of our process enriched with the developed extension of AD and DCA

The main objective is to enrich our process with the prior knowledge from a data stream whose objective is to design patterns to improve AD and DCA detection techniques with the necessary guidelines and prerequisites. This extension will facilitate fraud detection and also to address the research questions described in the previous section. An overview of this new extension of our process is given in Figure 2.

In our process, we have highlighted the necessary attitudes to integrate the features related to the mechanisms of strengthening the security aspect based on the prior knowledge. In fact, embeddings can be used to incorporate prior knowledge into learning models or learning profiles. Then, these embeddings will be considered as essential functionalities to ensure the detection of anomalies in systems based on machine learning and the semantic web, but it is necessary to proceed with a number of more concrete steps. However, the detection module is no longer enriched when the features vectors of the error signal no longer persist. Then, our previous process works based on a learning profile that uses embedded representations or knowledge graphs as technical prerequisites.

In this work, we have put all our efforts on the visualization and representation of useful knowledge. For this purpose, our process will take a matrix representation of knowledge graphs instead of using them in vector form due to embeddings techniques. In this representation, the rows represent subject-object, while the columns describe the types of relationship between these subjects and objects. With regard to the processing of this kind of representation, matrix analysis requires more computational effort, because the extractions scale linearly with the number of cells or thus the number of relationships or links within the knowledge graph. There is a high probability that useful data will be thrown and scattered all over the matrix. Therefore, our approach is based on the extraction of decisions from matrix representations by applying a series of adaptive and formals selections of a sequence of radiation regions. These radiation

regions project cells into the matrix that have relevant and valuable information about abnormal links.

However, how we choose the regions of radiation or interest describing the unwanted links. To answer this question, it was agreed on the human involvement to choose the sequence of interest in the suggested previous work in this discipline because, an excellent agent will be responsible for choosing from the region of radiation, and it will operate with partially available data. So, in the developed version of our process, we dedicated a rules-based virtual agent to accomplish the tasks of selecting regions of interest. We are talking about intelligent algorithms ensuring the automatic choice of interests in a matrix. This agent intervenes in order to automatically choose the necessary actions corresponds to the selected regions and also their location in the matrix. Therefore, our detection model will learn gradually based on experiences related to feedback from the processes of selection of regions of radiation and interest. Figure 3 describes in detail the improvements made to our process to take into account the generation of knowledge from matrix data. Therefore, the degree of accuracy of detecting links of undesirable anomalies in continuous increase, because the information extracted is based only on the links corresponds to the regions chosen in the matrix according to prior knowledge.

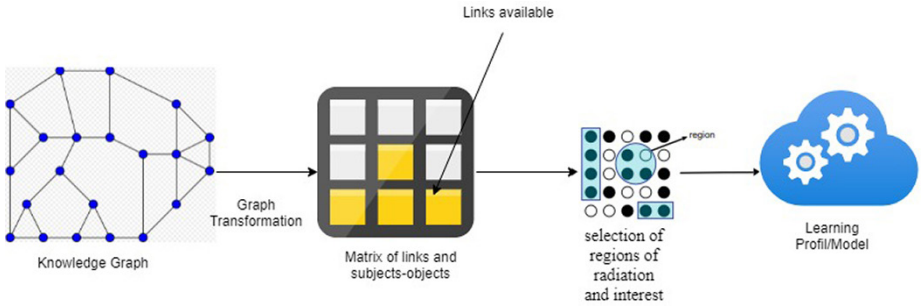

Fig. 3. Matrix knowledge learning process

We now describe how our process proceeds to generate the appropriate actions according to the features selected within the knowledge matrix. ML-based detection approaches begin by interpreting regions of interest. These approaches detect the links between the regions of interest representing the selected prior knowledge and the provided outcome. In this paper, we have projected the objects or characteristics of an object into features vectors in order to facilitate their processing on the one hand, and put them in a space of features where the decisions will be generated. In the Figure 4, show an example of a feature vector.

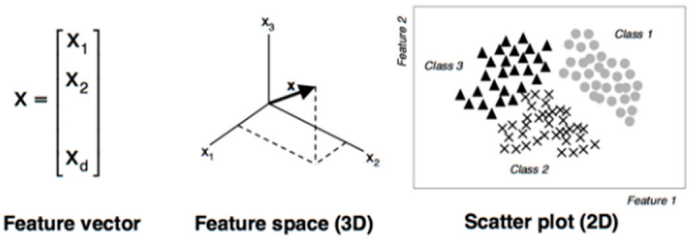

Fig. 4. Example of featue vector

This representation will allow us to provide a high level of interoperability and data interpretation, increasing the power to implicitly detect the causes and reasons behind unwanted system behavior. More precisely, it is the vector data comes from the embedded vectors, transformed in a graphical representation system, converted itself into a matrix, from which we reproduce valuable restrictions and strategies of use. For the transformation of vectors into graphs, there are as many methods previously proposed. For a reason of adaptability and quality, we have chosen Generative Adversarial Networks (GAN) to transform vectors into interpretable graph, from which we generate with conviction and precision the causes of an anomaly. The main idea is to convert the vector to graph by the generator of the GAN network, while the structures graph are consumed as inputs by the discriminate of the network. The discriminator proceeds to detect whether the data structure generated by the generating network is real or resembles part of the original knowledge graph. For this, we have updated the two constrictive networks of the GAN network until we have low number of faults generated. However, the discriminatory system finds it undeniable difficult to support and detect the difference between the original knowledge graph and that generated by the generator. An overview of such process is given in Figure 5. Finally, algorithms previously proposed in order to detect the cause behind the triggered anomalies using the embedded interpretation.

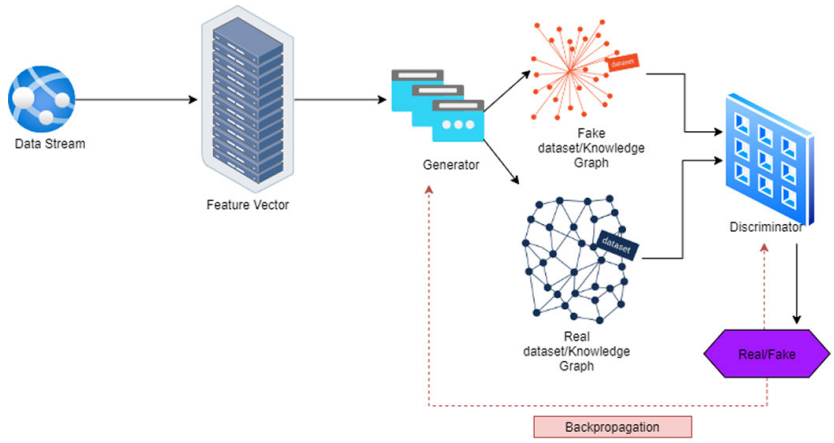

Fig. 5. Overview of our anomaly detection process using GAN

In this paper, we have integrated the consideration of real-time data against what is published in previous work. Concretely, we put a deep emphasis on data analysis and design in order to take into account the integration of knowledge into streaming data. In the literature, there are as many techniques ensuring the integration of knowledge graphs or valuable knowledge useful in a Data Stream. However, these techniques generate errors when a significant number of anomalies from different sources have occurred. To this end, human intervention is essential to activate the parameterization of this indisputable number of undesirable events. Design patterns are generated from the Data Stream based on machine learning, and used as embedded rules using machine learning to automate the process of detecting malicious events in a given system. These design patterns can be easily translated into numerical strategies and guidelines incorporated into the learning profile in order to reinforce it to take in addition to detection the estimation of the main causes causing convergence between the rules of use. Based on the interoperability and interpretation taken by our process, the design models derived from the Data Stream and design models previously negotiated in the literature, it has become so easy to convert these models to a set of rules. Specifically, the choice of design patterns is made automatically based on the complex event returned. Then, a set of data describing the guidelines of the chosen models will be made available to our learning model. Therefore, our process has the necessary attitudes allowing it to automatically choose the models and even the rules to be incorporated. In Figure 6, we describe how our process intercepts complex elements and derives the necessary rules.

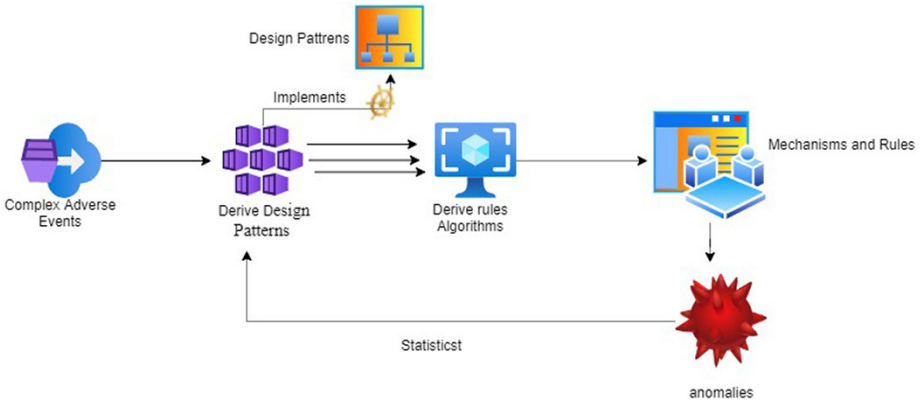

Fig. 6. Rules mechanisms generation

4 Results

In this work, we have the chance and the opportunity to highlight the virtual and logical difficulties blocking the processes of strengthening the optimization aspect in terms of qualification and integration of security policies and strategies in a mathematical space oriented by gigantic data. In the first step, we have clarified our process previously brought in this context to focus on the detection mechanisms using only the data itself to detect unwanted behaviour and actions. Secondly, we were able to

minimize minimise the large number of unwanted alarms and frauds generated disrupt the operation of the learning model, which destabilizes the frequency of accuracy. In Figure 7 we describe the results completed in this context.

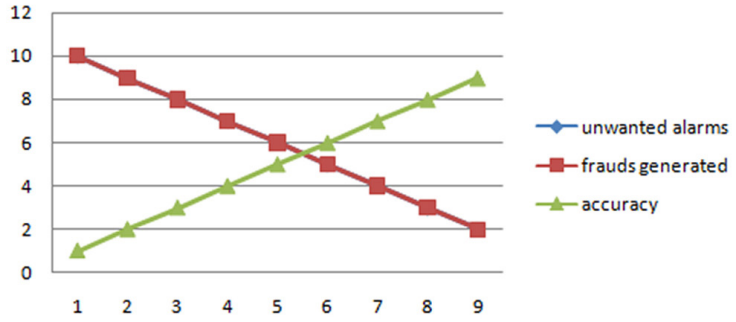

Fig. 7. Accuracy frequency of our learning model

Thirdly, our approach had focused on the AD and DCA methods in order to adapt them with coordinates and modifiable spaces unlike the old approaches proposed in these issues. As a result, we were able to make our process learning model capable of benefiting from changes in data and environments in real time. Fourthly, we were able to Increase by at least 4% false negatives and false positives by integrating prerequisites and prior knowledge. In Figure 8, we describe the results of our process.

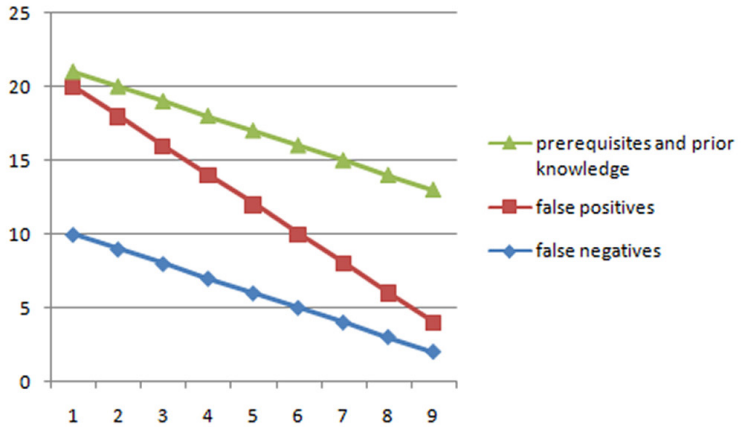

Fig. 8. Results of our process

Finally, we were able to reduce human involvement by more than 75%, in situations requiring a change of parameter in varying environmental contexts on the one hand, and. design a learning model applicable to streaming contexts, without causing a mixture of data by adapting our process to consider fraud detection and causes of errors in real time in different contexts.

5 Discussion

As described above in the previous axes, we have focused our efforts and focused on solving the problems given and negotiated in the literature such as:

- ✓ Current detection mechanisms using only the data itself to detect unwanted behaviour and actions.
- ✓ The large number of unwanted alarms and frauds generated disrupt the operation of the learning model, which destabilizes the frequency of accuracy.
- ✓ AD and DCA methods work with unchanged data, making it so difficult to process real-time data such as variable data and streaming contexts.
- ✓ AD and RCA's learning models are trained only once, making it impossible to consider change in the context of use so difficult, such as in streaming environments, sensor data and development in new contexts.
- ✓ The design of the RCA model requires a direct human involvement.
- ✓ Lack of evaluation and interpretation of decisions.
- ✓ The lack of self-adaptation of learning models with the change in settings of the deployment environment.
- ✓ Cover the lack of interoperability and data diversity

Therefore, our vision has enabled us to achieve the following goals:

- ➢ Adapt the learning and reasoning algorithms according to prior knowledge in order to achieve a detection rate exceeding by at least 2% the detection percentage of previously negotiated methods.
- ➢ Minimize 90% of unwanted signals and alarms causing malfunction in reasoning and learning models.
- ➢ Increase by at least 4% false negatives and false positives by integrating prerequisites and prior knowledge.
- ➢ Reduce human involvement by more than 75%, in situations requiring a change of parameter in varying environmental contexts.
- ➢ Design a learning model applicable to streaming contexts, without causing a mixture of data.
- ➢ Adapt our process to consider fraud detection and causes of errors in real time in different contexts.

6 Conclusion

In this work, we have proposed a new process of data manipulation while putting all our efforts on a well-defined engineering led by solutions already defined over time to resolve delicate situations related to the loss of big data, loss of semantics and meaning of data, difficulties in preparing data to value chain and lack of integrity. To do this, we began by defining the gaps and flaws that the field responsible for this kind of treatment suffers, and thus also identify all kinds of differences raised by all the work envisaged on this. It is also important not to forget the evolutionary criteria imposed by nature,

which themselves had an important factor behind what we were able to achieve and do. To this end, we proposed a new data preparation methodology focusing on the aspect of detecting anomalies and correcting errors in real time. This practice has allowed us to profile the experiences previously stored at the level of safety patterns. These guidelines have been leaked as data and are dedicated to resolving vulnerabilities related to anomalies detected during data manipulation. In such a way, and by applying our strategies defined at the level of the algorithms negotiated, we will have the power and resources necessary to design the machines involved the field of artificial intelligence capable of preventing the future in terms of anomalies, thus also the ability to build real-time solutions to detected anomalies.

From an economic point of view, we will prevent a 50 percent reduction in expenses compared to previous work. It should be remembered that we will produce gains of up to 40 percent improvement over current statistics.

As perspectives, we plan to add other technical details such as the one related to fault tolerance, the automation of the whole chain of big data, take into consideration the data storage criteria and model a repository guiding the data scientist and analyst to perform similar tasks without having an important required level in terms of the subject matter.

7 References

[1] Souiden, I., Brahmi, Z., & Toumi, H.: A survey on outlier detection in the context of stream mining: Review of existing approaches and recommadations. In: Madureira, A.M., Abraham, A., Gamboa, D., Novais, P. (eds.) ISDA 2016. AISC, vol. 557, pp. 372–383. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-53480-037; https://doi.org/10.1007/978-3-319-53480-0

[2] Solé, M., et al.: Survey on models and techniques for root-cause analysis. In: Clinical Orthopaedics and Related Research (CoRR), pp. 1–18 (2017).

[3] Lasbahani, A., Taoussi, C.: A new unsupervised learning-based process for extraction of knowledge's and improving anomalies detection. J. Phys. Conf. Ser. 2021, vol. 1743, 012024. https://doi.org/10.1088/1742-6596/1743/1/012024

[4] Ehsani-Besheli, F., Zarandi, H.R.: Context-aware anomaly detection in embedded systems. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.) DepCoS-RELCOMEX 2017. AISC, vol. 582, pp. 151–165. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-59415-6_15

[5] Huang, H., et al.: Streaming anomaly detection using randomized matrix sketching. Proc. VLDB Endow. 9(3), 192–203 (2015). https://doi.org/10.14778/2850583.2850593

[6] Jabeza, J., DR Muthukumar, B.: Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, vol. 48, pp. 338–346, 2015. https://doi.org/10.1016/j.procs.2015.04.191

[7] Ahmad, S., et al.: Unsupervised real-time anomaly detection for streaming data. Neurocomputing, vol. 262, pp. 134–147, (2017). https://doi.org/10.1016/j.neucom.2017.04.070

[8] He, Y., et al.: Mechanism-indepedent outlier detection method for online experimentation. In: IEEE International Conference on Data Science, pp. 640–647 (2017). https://doi.org/10.1109/DSAA.2017.64

[9] Ademujimi, T. T., Brundage, M. P., & Prabhu, V. V. (2017). A review of current machine learning techniques used in manufacturing diagnosis. In R. Riedel, K-D. Thoben, D. Kiritsis, G. von Cieminski, & H. Lodding (Eds.), Advances in Production Management Systems: The Path to Intelligent, Collaborative and Sustainable Manufacturing—IFIP WG 5.7 International Conference, APMS 2017, Proceedings (pp. 407–415). (IFIP Advances in Information and Communication Technology; Vol. 513). Springer New York LLC. https://doi.org/10.1007/978-3-319-66923-6_48

[10] Smith, B.A., et al.: Fault diagnosis using first order logic tools. In: Proceedings of the 32nd Midwest Symposium on Circuits and Systems, vol. 1, pp. 299–302, August 1989. Zheng, A.X., et al.: Failure diagnosis using decision trees. In: Proceedings of the First International Conference on Autonomic Computing (2004).

[11] Berners-Lee, T., Hendler, J., & Lassila, O.: The semantic web. Sci. Am. 284(5), pp. 34–43 (2001). https://doi.org/10.1038/scientificamerican0501-34

[12] Paulheim, H., et al.: Exploiting linked open data as background knowledge in data mining. In: International Workshop on Linked Data, pp. 1–10 (2013).

[13] Nguyen, D.Q.: An overview of embedding models of entities and relationships for knowledge base completion. arXiv preprint arXiv 1703.08098 (2017).

[14] Schlichtkrull, M.S., et al.: Modeling relational data with graph convolutional networks. CoRR abs/1703.06103 (2017).

[15] Camossi, E., et al.: Semantic-based anomalous pattern discovery in moving object trajectories, pp. 1–20. CoRR abs/1305.1 (2013).

[16] Solé, M., et al.: Survey on models and techniques for root-cause analysis. In: Clinical Orthopaedics and Related Research (CoRR), pp. 1–18 (2017).

8 Authors

Abdellatif Lasbahani, Laboratory EMI, University Sultan Moulay Slimane, Beni Mellal, Morocco.

Rachid Tahri, Faculty of Sciences and Techniques, Hassan First University, Settat, Morocco.

Abdessamed Jarrar, Faculty of Sciences, Mohammed First University, Oujda, Morocco.

Youssef Balouki, Faculty of Sciences and Techniques, Hassan First University, Settat, Morocco.

Article submitted 2022-02-08. Resubmitted 2023-01-22. Final acceptance 2023-01-23. Final version published as submitted by the authors.