Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

ICSC
Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing

ISP – Fraud Detection

Spoke 2 Workshop, Bologna Dec 19 /12, 2023

Scientific Rationale

In finance, **fraud detection** is an extremely important form of anomaly detection. Some examples are identifying **fraudulent credit card transactions** and **financial documents**. These tasks are typically performed using **supervised** or **unsupervised** deep learning.

Over the past few years, the financial industry has seen substantial growth in innovation, particularly in the field of **AI/ML** for the payment industry to keep fraud losses contained. The current challenges are those of finding the balance between the false positives that, if too common, could serve as a **negative impact** on a **client's experience** and **minimizing the monetary loss** incurred by fraudulent transactions. Yet **criminals** are also constantly increasing their **capabilities** to deploy ever **more complex fraud schemes** at a rate difficult to keep up. Many have started using AI/ML to augment the efficacy of their attacks. The payment industry defends itself in multiple ways: more data from more sources is used, more behavioral features are extracted as inputs to the AI/ML models, and better machine learning models.

Technical Objectives, Methodologies and Solutions

1° delivery Dataset - description

There is already a Dataset ready to be used in the experimentations, composed of **515651 rows** and **17 columns**.
The dataset represents synthetic data based on **real transactions** alerted by **Intesa Sanpaolo** Transaction Monitoring Engine.
The data format is CSV. The data represents a sample of transactions that occurred during the year 2022.
Sensible information has been hashed with the **SHA-512 algorithm**.
The **first column**, defined by the description “chiave_univoca”, is the **transaction ID**.
The **second column** represents the transaction event **timestamp**.
The **third column** represents the economic **amount** of the transaction.
Columns from **fourth to sixth** represent the **year**, **month**, and **day**. The **seventh** column represents the **target** for the supervised learning task.
The target is a **binary variable**, where a **fraudulent transaction** is encoded with **1** and a **genuine transaction** is encoded with **0**.
The dataset is **highly imbalanced** i.e., ratio around **2%**. The **remaining columns** represent hashed **categorical features** of the transactions.
The data can contain **missing values**, that should be treated in the pre-processing phase.

Coming soon: time series dataset

Timescale, Milestones and KPIs

The work package in the Spoke 2 corresponds to WP3 and 2.

Deliverable:

- M6 Data delivery – completed 100%
- M7 Preliminary results on data exploration and how to format the dataset, preprocessing the data (e.g. feature engineering, feature selection) - completed 0%
- M8 first prototype application with ML to one use case – completed 0%
- M9 Prototype with explainability - completed 0%
- M10 Python library that works on the banking dataset and environment – completed 0%

Timescale, Milestones and KPIs

The work package in the Spoke 2 corresponds to WP3 and 2.

Deliverable:
M7 Preliminary results on data exploration and how to format the dataset, preprocessing the data (e.g. feature engineering, feature selection)

In the initial stages of the project, the team undertook several critical actions to prepare the data effectively. They began by conducting preliminary data exploration, delving into the dataset to gain insights and identify patterns. Simultaneously, they worked on formatting the dataset, ensuring it was organized and structured in a way that would facilitate further analysis. Additionally, they engaged in preprocessing the data, a multifaceted task that encompassed activities such as feature engineering and feature selection. These efforts were aimed at refining and enhancing the dataset, optimizing it for subsequent machine learning and analytical tasks.

Need: kick-off meeting with counterparts for defining the technical objective and sharing the data.

KPI: 2x100. Link experiments and methods for data exploration and/or preparation in a repository. Measure: 100% present, 0% not delivered. 1 h presentation of the discovery and the data preparation (ppt, technical report?). Measure: 100% done, 0% not done.

Timescale, Milestones and KPIs

The work package in the Spoke 2 corresponds to WP3 and 2.

Deliverable:

M8 first prototype application with ML to one use case. Prepare paper to submit

The team commenced the project by developing the M8 prototype application, incorporating machine learning techniques to address a specific use case. They constructed a solution informed by the extensive expertise and domain knowledge of their counterparts, ensuring a highly specialized and effective approach.

Project written in Python in a Git environment, commented, modular (developed in class) such that the pipeline could consist in:

1. DF = Data_preparation(data, ...)
2. M = Train_model(DF, develop=False, ...)
3. M.predict(DF)

KPI: 2x100. Working code in the Git repository: done 100% otherwise 0%. Tutorial 1h presentation 100%, 0% otherwise.

Timescale, Milestones and KPIs

The work package in the Spoke 2 corresponds to WP3 and 2.

Deliverable:
M9 Prototype with explainability. Submit paper to be reviewed
represents a significant advancement, as it not only showcases the prototype's functionality but also emphasizes the crucial aspect of interpretability, enabling a deeper understanding of the machine learning models' decision-making processes.

Add in pipeline:
1. M.explain(sample)

KPI: 2x100. feature implemented (or present by design) 100%, not implemented 0%. Submission of the paper to a journal/high-level-conference 100%, 0% otherwise.

Timescale, Milestones and KPIs

The work package in the Spoke 2 corresponds to WP3 and 2.

Deliverable:
M10 Python library that works on the banking dataset and environment.
The M10 Python library has been designed to operate seamlessly within the banking dataset and environment, facilitating robust and tailored data analysis and processing.

pip install coolestProject

```
CoolestProject.prepare_dataset()
CoolestProject.train()
CoolestProject.predict()
CoolestProject.explain()
```

KPI: 4x100. if NAME SURNAME can install it on his PC and use it on a toy dataset 100%, 0% otherwise. Quick start on GitHub page 100%, 0% otherwise. Documented page on GitHub (readthedocs) 100%, 0% otherwise. Paper published in a journal/high-level-conference 100%, 0% otherwise.

Timescale, Milestones and KPIs

UNIPD - Marco Zanetti

The **search** for **anomalies** is an area in which considerable progress progress have been realized in recent years, with the contribution of different disciplines; in particular, developing and putting in production of algorithms for searching for **signals** that **deviate from theoretical predictions** is one of the main objectives of the modern experimental physics.
The research group of the Department of Physics of the University of Padova, in collaboration with colleagues of CERN and other research centers, has designed and developed a **anomaly detection algorithm** (New Physics Learning Machine, NPLM [padova1]) which exploits **universal approximators** (neural networks, kernels, etc.) **to compare the collected data with the respective expectations**, effectively identifying deviations from the latter, describing them the essential characteristics.
This algorithm has also been applied to the **detection of anomalous transactions** in the data relating to purchases made through **credit cards** [padova2], with excellent results. The peculiarity of this method consists **not in classifying as legitimate or not a single treatment** (classification), but in **detecting in a set of transactions** if some of them **deviate from the "normal"**. Unlike
classical classification, **NPLM** need not know in advance the anomaly - i.e. the type of fraud -, the method is therefore particularly **robust** against as **yet unidentified fraud**.

[padova1] https://inspirehep.net/literature/1977309
[padova2] https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

Timescale, Milestones and KPIs

UNIFI - Piergiulio Lenzi

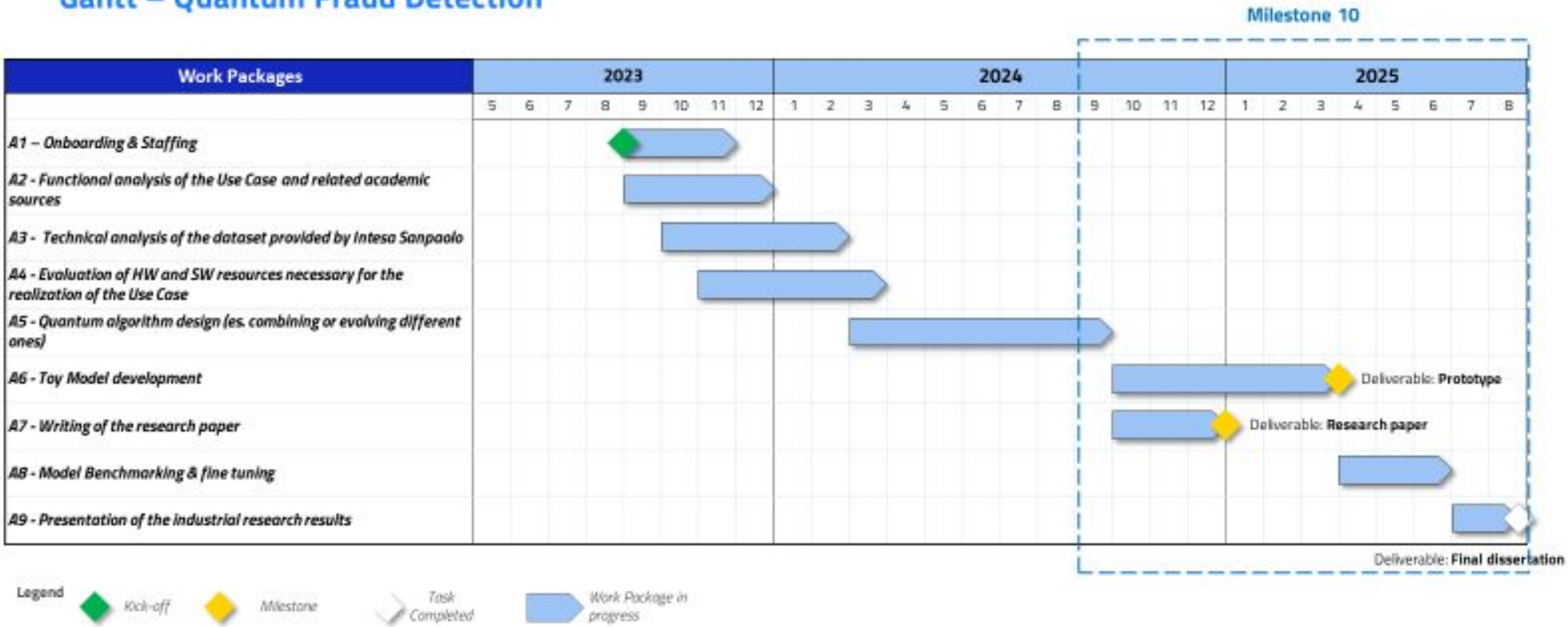
We propose the use of **autoencoders for anomaly detection** in the transactions, using **LSTM** layers. As mentioned in the project, **false positives are a challenge**, and it is also important to ensure that false positives do not affect in an uneven fashion different types of transactions. For example, it would be desirable that the **probability of false positives** per transaction **is flat with respect to the number of transactions**, or to the volume of transactions (for example avoid that someone with a high transaction rate has a false positive probability per transaction that is different from someone with a lower transaction rate. Same for volume).
We plan to address this issue with a combination of **feature engineering** and **adversarial approaches**, in which the **autoencoder** has a **regressor** adversary which tries to regress the feature with respect to which we want to be independent.

Timescale, Milestones and KPIs

INAF Palermo - Antonio Pagliaro

proposed approach involves implementing **Stacking Ensemble Learning**, which combines predictions from multiple base classifiers, including Random Forest (RF), Extra Trees, and XGBoost (XGB), to improve **fraud detection** in the payment industry.
The Stacking Ensemble Learning model will utilize these base **classifiers**, combining their predictions to make the final fraud detection decision. The model will leverage diverse data sources, **extracting relevant behavioral features** to capture fraud patterns effectively.

Gantt – Quantum Fraud Detection



Next Steps and Expected Results (by next checkpoint: April 2024)

Fraud Detection:

- On a small scale, we aim to achieve a more precise automated detection of fraud, leading to a better customer experience, and a decreased monetary loss for the company.
- On a larger scale, by better intercepting fraud in our financial transactions, we could increase our commitment to the National and European supervisory authorities, reinforcing their capabilities in the fight against financial crimes.
- For Fraud Detection reduce the False Positive by 10% of the standard process (XGBoost of features extracted from the TS).
- Reducing False Positive avoids inconvenience related to the interruption of customer operations, and thus increasing customer satisfaction and preventing reputational damage.
- Moreover, the environmental footprint of quantum computation is less demanding compared to HPC data centers that are generally used to address this kind of problem.