



**HAL**  
open science

## Multiples inputs neural nets for Medicare fraud detection

Mansour Zoubeirou a Mayaki, Michel Riveill

► **To cite this version:**

Mansour Zoubeirou a Mayaki, Michel Riveill. Multiples inputs neural nets for Medicare fraud detection. SOPHIA SUMMIT 2021, Nov 2021, Sophia Antipolis, France. hal-03851634

**HAL Id: hal-03851634**

**<https://hal.science/hal-03851634>**

Submitted on 14 Nov 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Sofia Summit 2021 conference

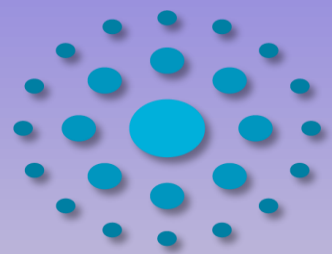
17-19 November 2021  
Sophia Antipolis, France

## **Multiples inputs neural nets for Medicare fraud detection**

**Mansour ZOUBEIROU A MAYAKI and Michel RIVEILL**

Phd student, Université Côte d'Azur, CNRS, Inria, I3S, France

Team: MAASAI



UNIVERSITÉ  
CÔTE D'AZUR

01 Medicare fraud

02 Fraud detection systems

03 What is machine learning: artificial neural nets

04 Imbalance class challenge

05 Our model's architecture

06 Experimental results

01

### What is Medicare fraud:

- billing for appointments that the patient did not keep,
- billing for services more complex than those performed
- billing for services not provided
- billing for unnecessary medical services etc...

02

**In Europe:** 13 billion euros per year to European citizens

03

**In France :** over 200 billions € public spends per year

- 2018 => 261,2 millions €
- 2019 => 287 millions €
- At least 2.4 billions since 2005

04

### Consequences:

- increase in public funds/Mutual
- Causes an imbalance between contributions and benefits.
- increase in contributions
- interferes with the efficiency of the care of customers who really need it

# FRAUD DETECTION SYSTEMS

01

## Manual reviews

- slow
- time-consuming
- often unnecessary.

02

## Rules based

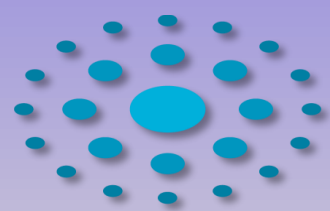
- uses correlation and logical comparison of data to identify potential fraud based on insights gained from previous (known) fraud incidents. traditional
- They generally use methods of data analysis
- require complex and time-consuming investigations that deal with different domains of knowledge like financial, economics, business practices and behavior.
- Difficult to update: new fraud pattern, new laws etc.

03

## Machine Learning based

- identifies suspicious patterns and behaviors
- analyze clients current patterns and transaction methods.
- It can analyze these behaviors faster and more efficient than any human analysis and as a result, it can quickly identify if there is a deviation from normal behavior.
- The final decision is made by human expertise

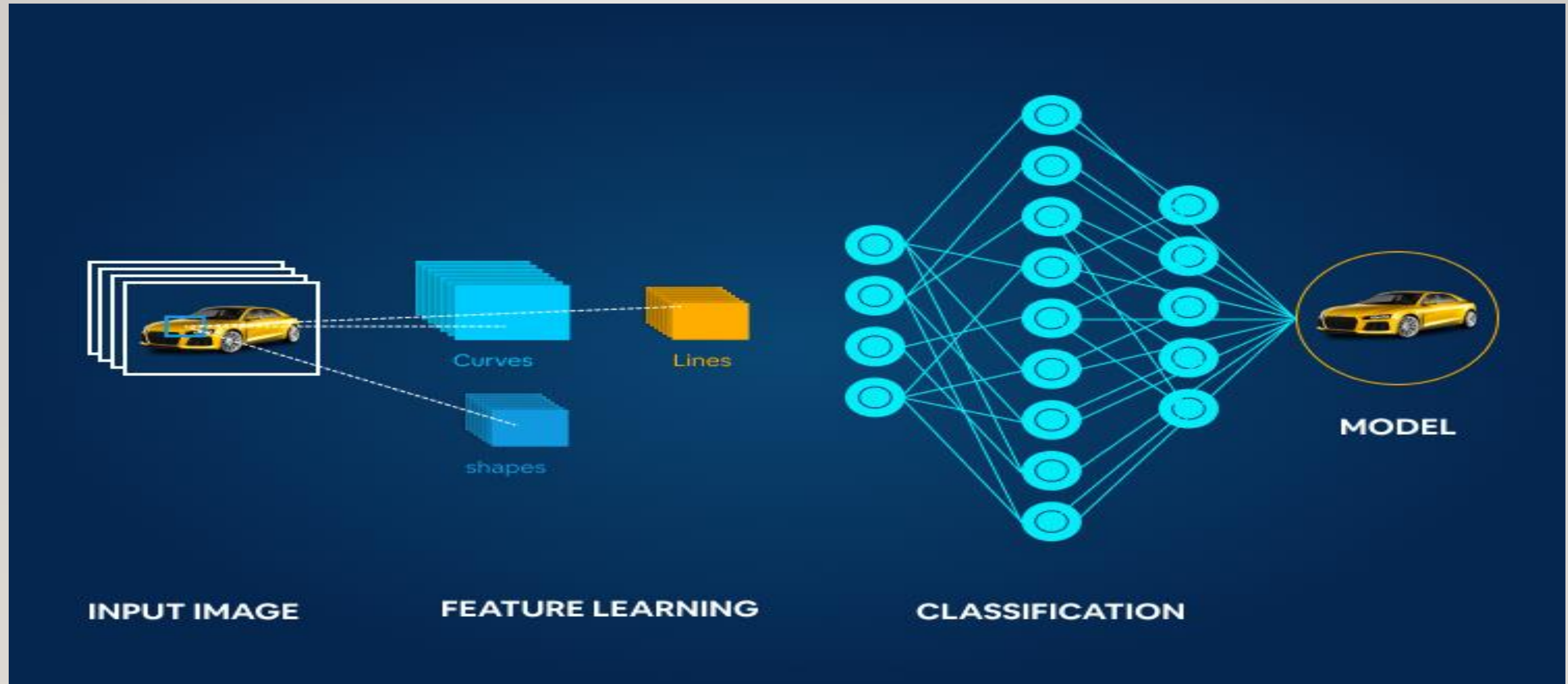
# Machine Learning



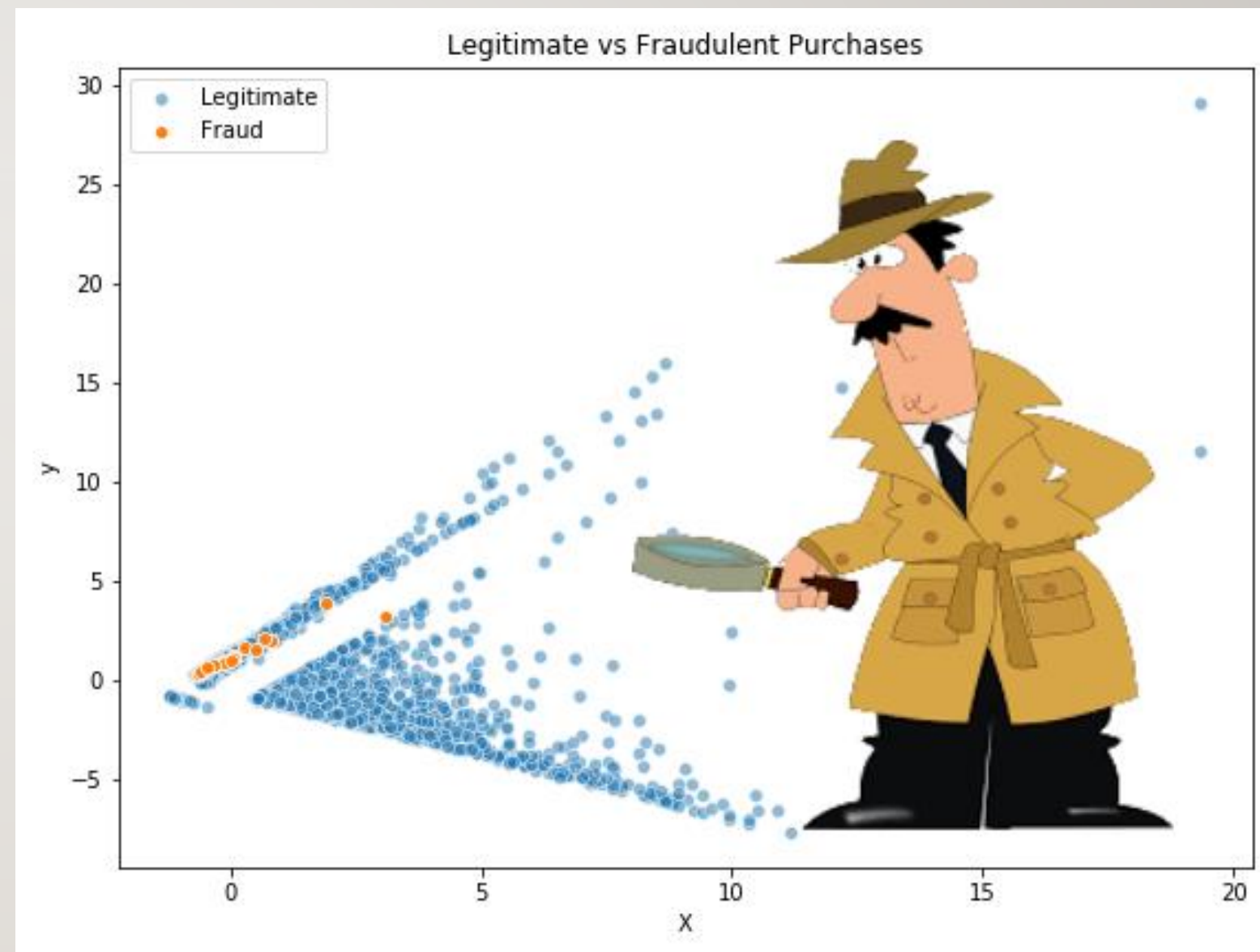
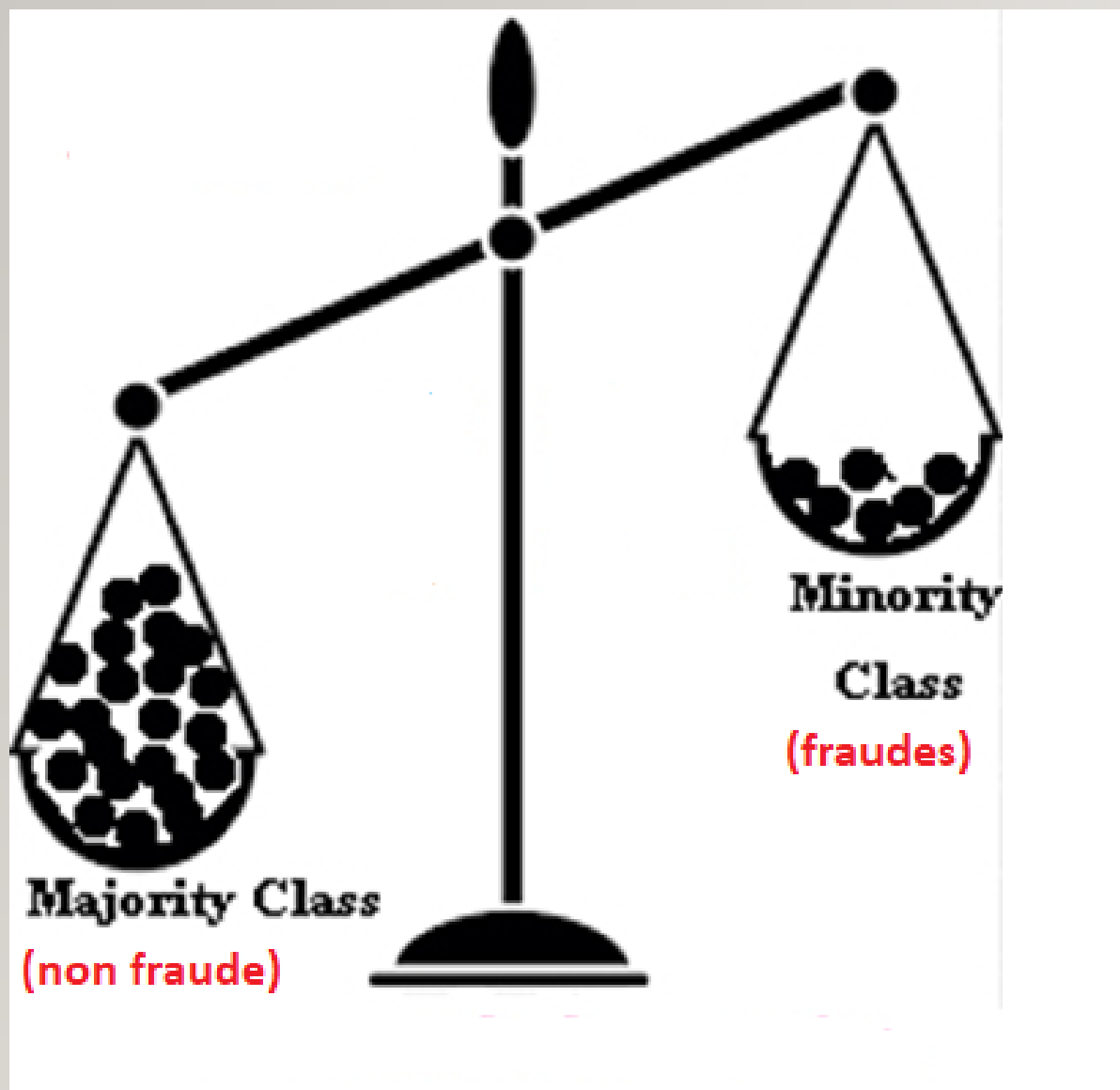
UNIVERSITÉ  
CÔTE D'AZUR



# ARTIFICIAL NEURAL NETS FOR FRAUD DETECTION



# IMBALANCE DATA CHALLENGE



Data level methods: random oversampling (ROS), random undersampling (RUS)

Algorithm level methods: Weighted loss, Focal loss, Etc.



# CMS DATA

01

Origin: Centers for Medicare & Medicaid Services (CMS)

02

Inpatient Data : information on patients admitted to hospitals

03

Outpatient Data : information on patients who have visited the hospital without being hospitalized there

03

Beneficiary Details Data: contains data on the patient's state of health and socio-demographic characteristics (age, sex, place of residence, etc.)

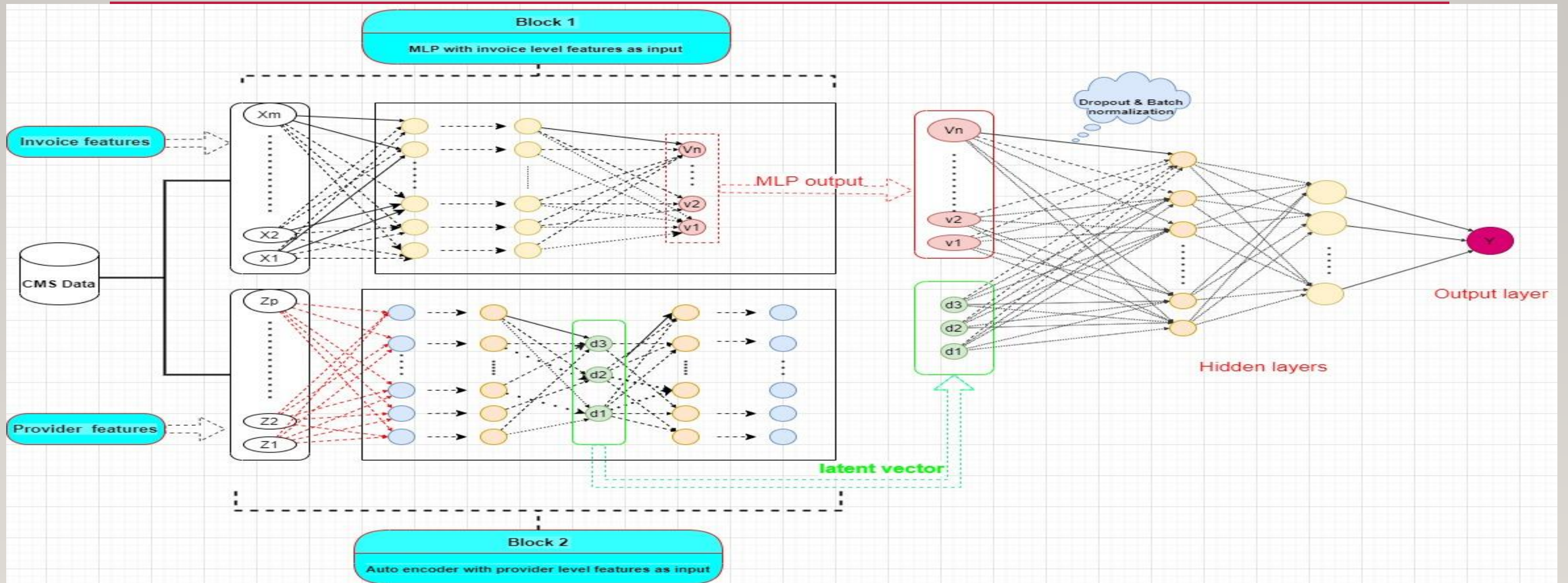
03

Outpatient Data : information on patients who have visited the hospital without being hospitalized there

**Table 3:** Data aggregated provider level

Provider	BeneID_count	DeductibleAmtPaid_mean	InscClaimAmtReimbursed_sum	BeneID_count_trim1	PotentialFraud
PRV51001	24	213.60	104640	8.0	No
PRV51003	117	502.16	605670	39.0	Yes
PRV51004	138	2.08	52170	48.0	No
PRV51007	58	45.33	33710	20.0	No
PRV51008	36	53.86	35630	11.0	No

# Our model's architecture



# EXPERIMENTAL RESULTS

Table 5: Experimental Results

Models	TPR (Recall)	ROC AUC	Gmeans-score	TN rate score
LR	0.829	0.849	0.849	0.870
RF	0.568	0.769	0.742	0.971
GB	0.401	0.692	0.628	0.984
MLP [9]	0.783	0.821	0.818	0.859
MLP weighted [9]	0.823	0.836	0.833	0.850
MLP focal [11]	0.845	0.815	0.810	0.785
MLP mfc [18]	0.847	0.859	0.857	0.870
ROS [10]	0.726	0.806	0.801	0.886
MINN AE	0.863	<b>0.876</b>	0.876	0.890



Our model outperform the other classifiers:

- Best AUC
- Best recall
- Best G-means



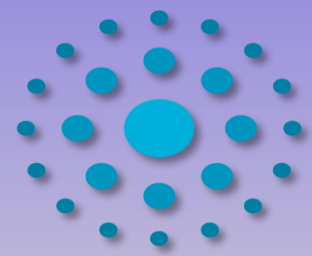
## Highlights:

- Takes into account the provider level features
- Separate sources of information
- Robust to data imbalance:
  - The latent features have strong clustering power that makes it easier to classify fraudulent invoices

We need enough historical data to model the provider behavior: can be difficult for a new provider



**Thank you for your  
attention**



UNIVERSITÉ  
CÔTE D'AZUR

