**School of Computational Sciences and Artificial Intelligence Information Theory**


# *Card Fraud Detection Based on CatBoost*

*By*

**Ahmed Kahla 202202231**

**School of Computational Sciences and Artificial Intelligence Information Theory**


# Model

The project implements the hybrid model described in the paper "*A Proposed Model for Card Fraud Detection Based on CatBoost and Deep Neural Network.*"
The paper divided the users into new users and old users, then implemented Catboost model on the new users, and Deep neural network model on the old users. The paper uses SMOTE for addressing class imbalance problems while XAI techniques provide explanations of model outputs. The first part of implementation concentrated on creating CatBoost components from the hybrid model through use of identical essential procedures. CatBoostClassifier with tuned hyperparameters.
The algorithm applies SMOTE to provide additional samples of minority cases (fraudulent transactions) during the sampling procedure. The paper applied Evaluation metrics consisting of Precision, Recall, AUC, and Accuracy as described in the paper.

# Feature Selection

We applied univariate feature selection (forward selection), forward selection technique aligning with the paper in order to reduce input dimensionality and remove the noisy features.
The function SelectKBest(K = 6) is selecting the most 6 informative features that is related to the target class.
After extracting the names of the top 6 features, we built a smaller dataframe that is contain these 6 features with the target column.
This feature selection step effectively:

- Reduced the dimensionality of the dataset
- Improved model training speed
- Helped mitigate potential overfitting
- Made the model more explainable

The paper used trained CatBoost models through selected features that employed a concept similar to the one presented in the paper (e.g., dimensionality reduction via PCA on the IEEE-CIS dataset).
In our case the (creditcard.csv dataset) we selected important features through use of SelectKBest given that the dataset is small and its V1–V28 features are already transformed.

**School of Computational Sciences and Artificial Intelligence Information Theory**


## XAI Techniques Used

One of the key points the paper highlights is the need for explainability in fraud detection. It's not just about building a model that works it's about making sure we understand why it makes the decisions it does. That's especially important in real-world scenarios where financial institutions need to justify or investigate flagged transactions.

To start moving in that direction, I've included interpretability tools in my evaluation process:

**Confusion Matrix:** This gives a quick, visual snapshot of how well the model is doing. It shows how many fraud cases it caught correctly and where it made mistakes.

**Performance Metrics:**

- **Precision** tells us how many of the flagged frauds were actually fraud.
- **Recall** shows how good the model is at catching all the fraud cases.
- **Accuracy** gives us the overall correctness of the model.
- **ROC-AUC** gives a broader view of how well the model can separate fraud from non-fraud over different thresholds.

## Results

**Accuracy: 98.18%**

The model demonstrates success in correctly identifying most transactions throughout the dataset. The model successively detects real instances of fraud while achieving a much higher detection rate.

**Precision: 0.068**

The precision score reveals that the model identifies more fraud cases but mistakenly marks many valid transactions as fraudulent. The model correctly identifies fraud cases only 6.8% of the time when it declares something fraudulent. The system opts for caution by producing additional unneeded alerts rather than taking risks with actual fraud detection.

**Recall: 0.82**

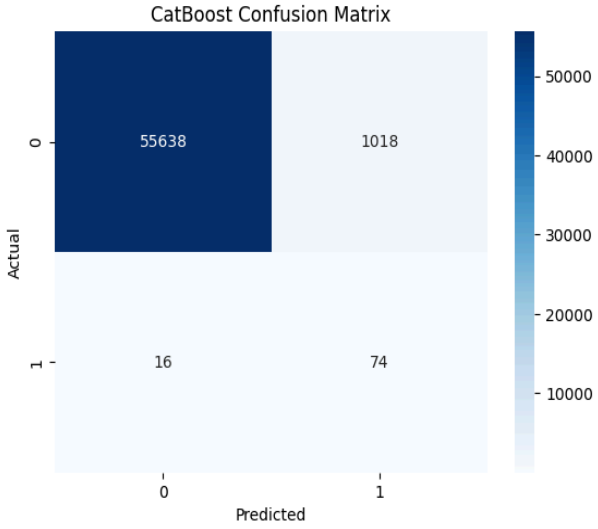
The model shows its best performance in this part. The system successfully detected 82% of all fraudulent activities proving its effectiveness. The detection of fraud becomes more critical than the prevention of legitimate transactions when it comes to detecting fraudulent behavior.

**ROC-AUC: 0.94**

The model demonstrates its ability to differentiate between fraudulent and legitimate activities across different decision threshold points through this score. The model demonstrates meaningful pattern learning in the data through its high scoring ability.

## School of Computational Sciences and Artificial Intelligence Information Theory

### Confusion Matrix:




**True Positives (Fraud correctly detected): 74**
The model successfully detected all instances of fraud which represents successful outcome.
**False Negatives (Fraud that slipped through): 16**
Only 16 fraud cases were missed. The detection rate of fraud represents a solid outcome considering its difficult nature.
**False Positives (Legitimate transactions flagged as fraud): 1,018**
The model achieves better fraud detection yet creates a problem by misidentifying more than one thousand legitimate transactions.
**True Negatives (Legit transactions correctly passed): 55,638**
The model successfully identified most regular transactions which demonstrates its strong performance capability.