Enhance Credit Card Fraud Detection Using Generative AI

Course: CSC 496 – Graduation Project
Supervisor: Dr. Amani Alajlan

Presented by: Fai Alharthi, Shoug Alsaleem, Lina Alsuwaylimi, Raghad Aldosari, Aliyah Aljarallah

What is Fraud Detection?

process of identifying and preventing unauthorized or suspicious activities, especially in financial transactions like credit card payments.

Problem Statement

- Fraud cases are extremely rare .
- Severe class imbalance in data.
- Traditional models struggle to detect rare cases.
- High chance of false positives or missed fraud.

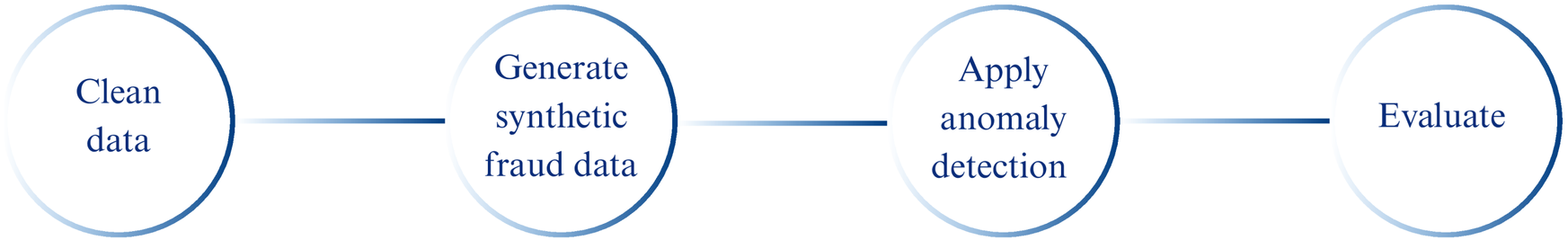
Goals & Objectives

The goal is to build an intelligent system that can accurately detect credit card fraud and reduce false alarms, especially in cases where fraudulent transactions are very rare.

Objectives:

- Review related research
- Use a public credit card transaction dataset.
- Generate synthetic fraud data using GANs.
- Apply models
- Evaluate performance

Our Solution



Class Imbalance

Class Imbalance Problem

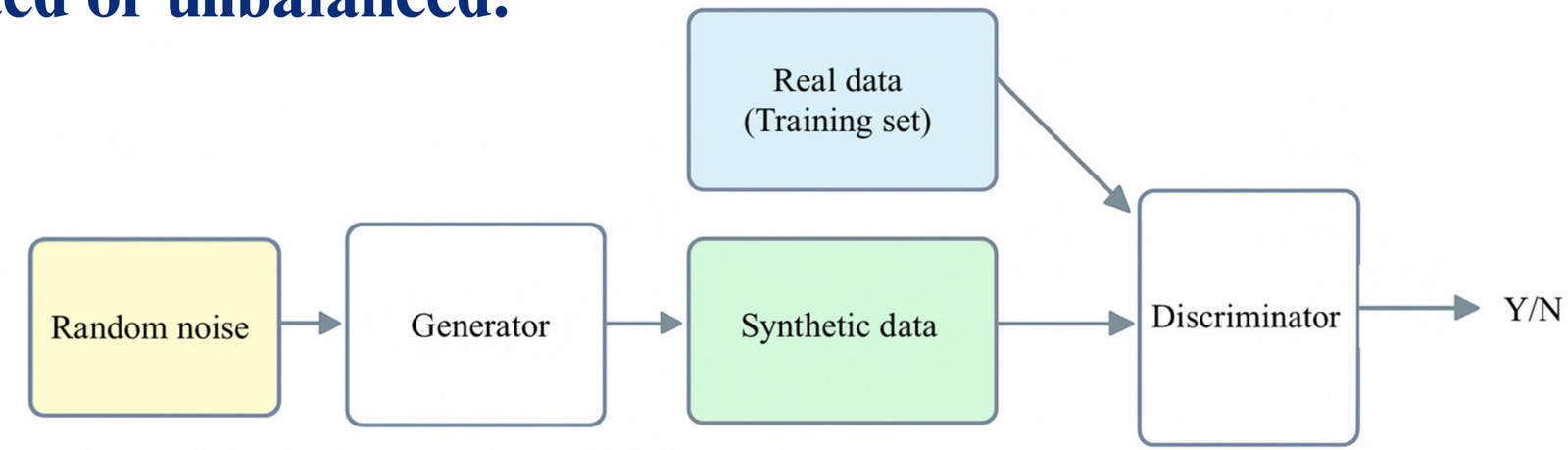
- Most credit card transactions are normal.
- Fraud cases are very rare
- This imbalance makes it hard for models to learn fraud patterns.
- Exists in many fields

Role of Generative AI

- We use GANs to generate synthetic fraud data
- This helps balance the dataset and improve detection.

Generative Adversarial Networks (GANs):

- **Two parts:**
  - Generator: creates synthetic data.
  - Discriminator: checks if it's real or not.
- **Useful when data is limited or unbalanced.**



VAE & Diffusion Models

Variational Autoencoder (VAE)

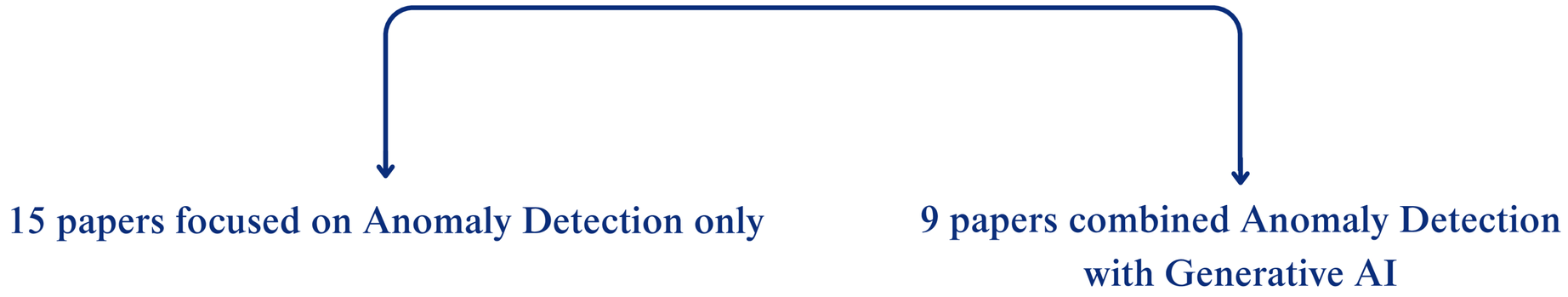
- Generates varied and realistic fraud data
- Learns patterns to avoid duplication

Diffusion Models:

- Add and remove noise to create synthetic samples
- More stable than GANs, with better accuracy

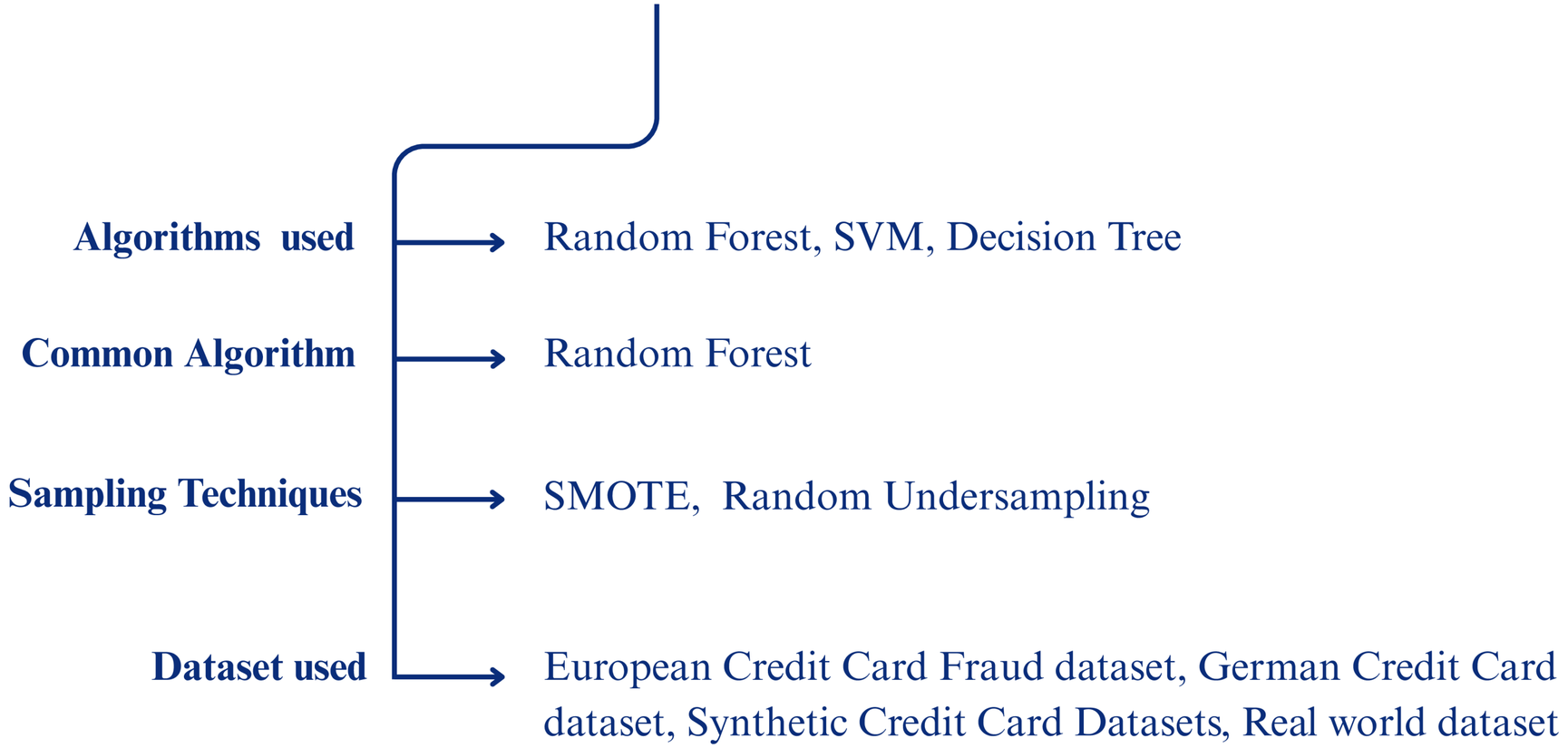
Literature review

We reviewed and compared a total of 24 papers on credit card fraud detection



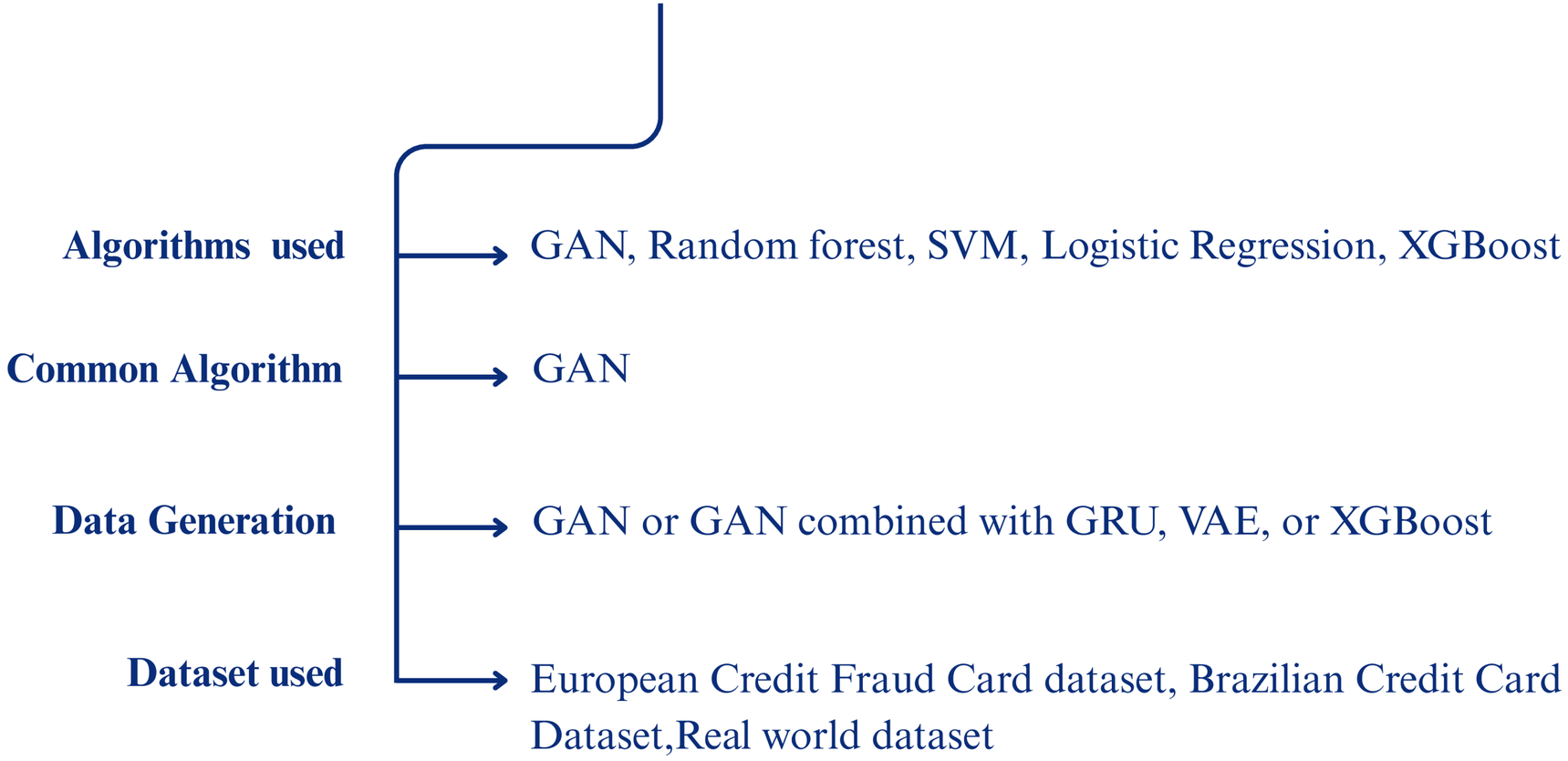
Literature review

Anomaly Detection Studies



Literature review

- **Anomaly Detection + Generative AI Studies**



Dataset overview

➢ European Credit Card Fraud

Feature	Type	Description
Time	Numerical	Time in seconds since the first transaction
Amount	Numerical	Value of the transaction in euros
V1 to V28	Numerical	PCA-transformed anonymous features
Class	Categorical	Target label: 0 = normal, 1 = fraud

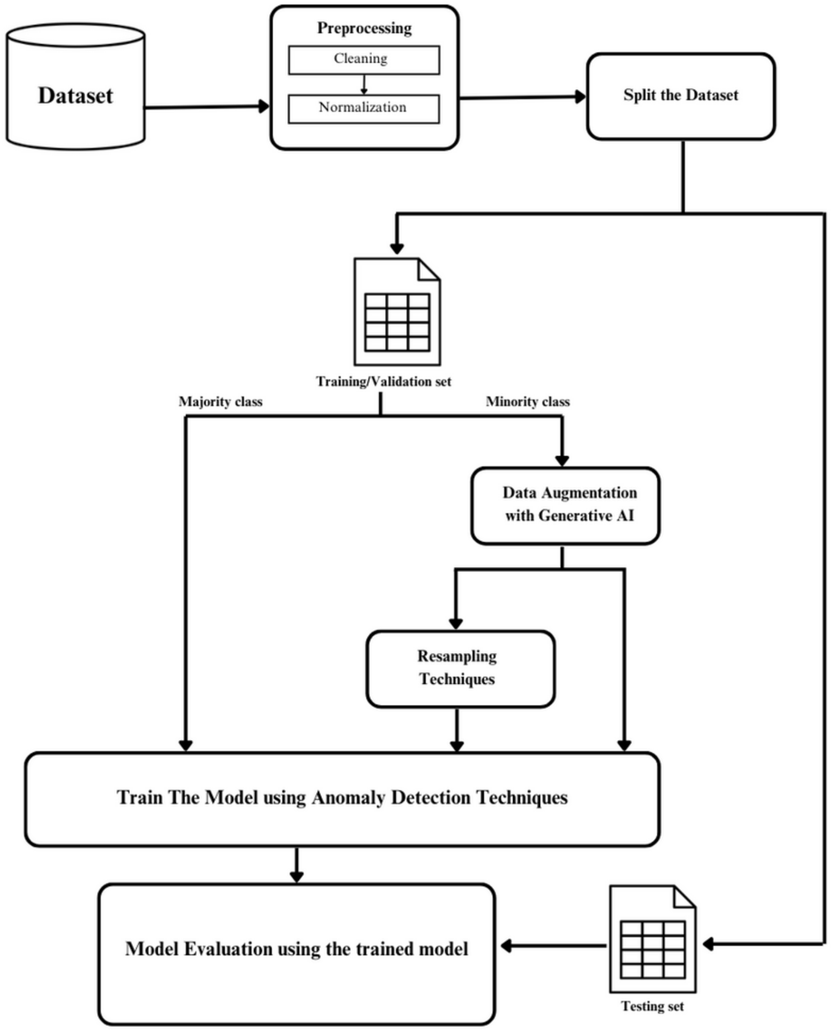
Dataset overview

European Credit Card Fraud

Total transactions: 284,807 | Fraud cases: 492 (0.17%)

	Time	V1	.....	V28	Amount	Class
1	0	-1.3598071336738		-0.0210530534538215	149.62	0
	⋮					
284,807	17279	-0.53341252200504		0.0136489143320671	217	0

Overview of the Methodology

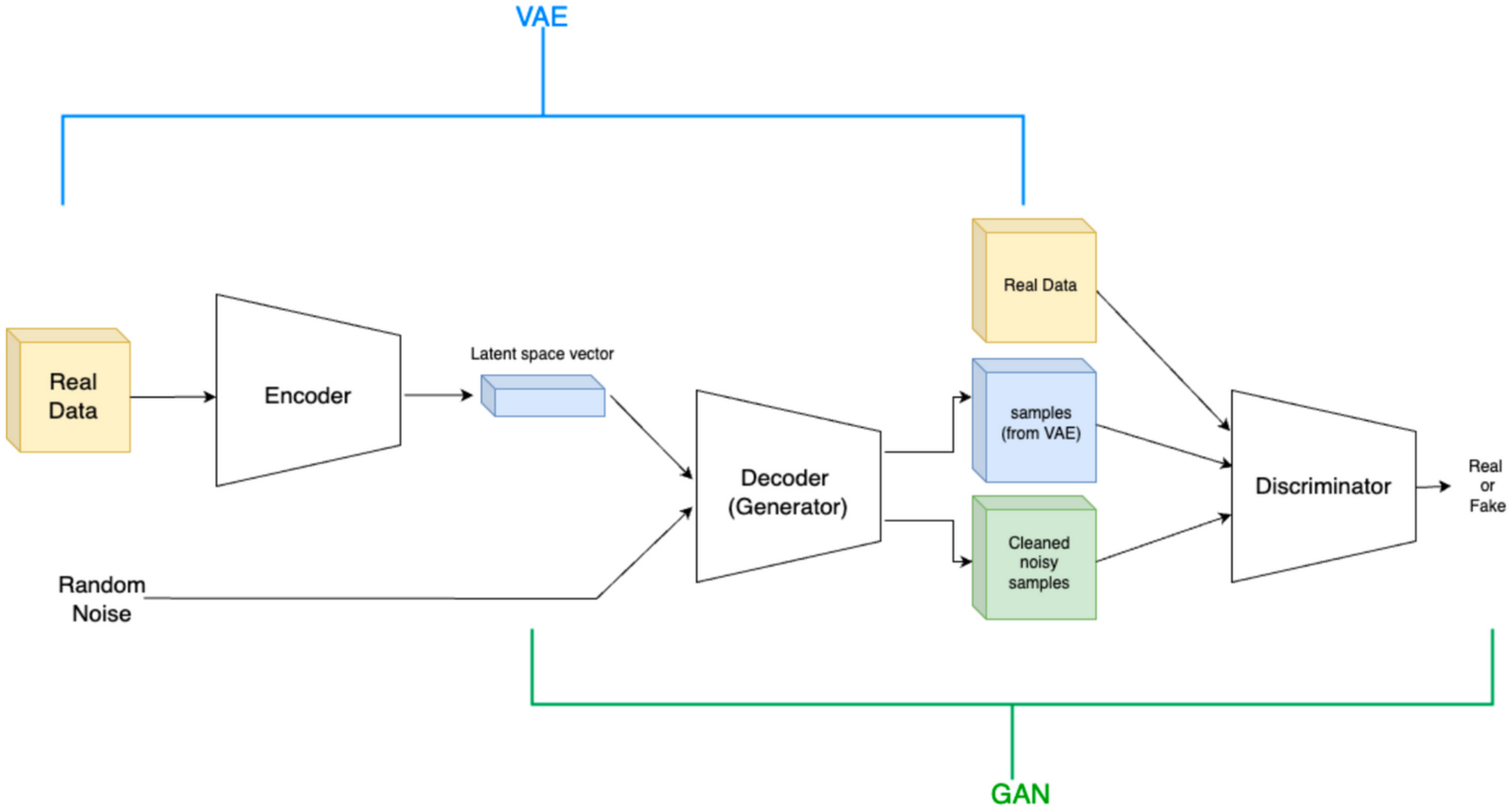


Key Components:

- Preprocessing
- Data Division
- Data Augmentation
- Resampling Technique
- Anomaly Detection
- Model Evaluation

Data Augmentation with Generative AI

- VAE-GAN Model

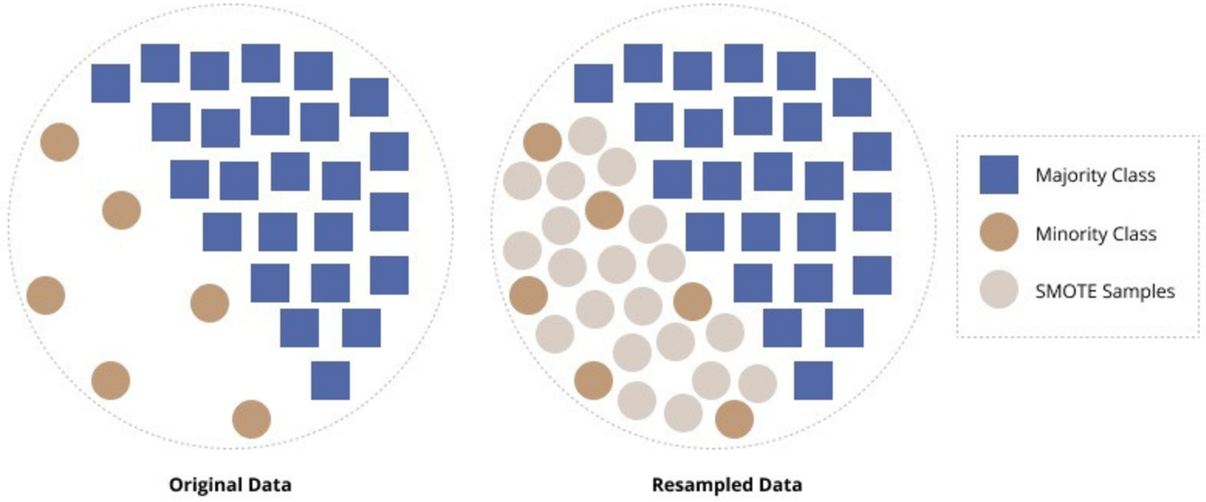


Resampling Technique

➢ SMOTE stands for Synthetic Minority Over-sampling Technique.

Instead of duplicating existing fraud cases, SMOTE generates new synthetic samples by:

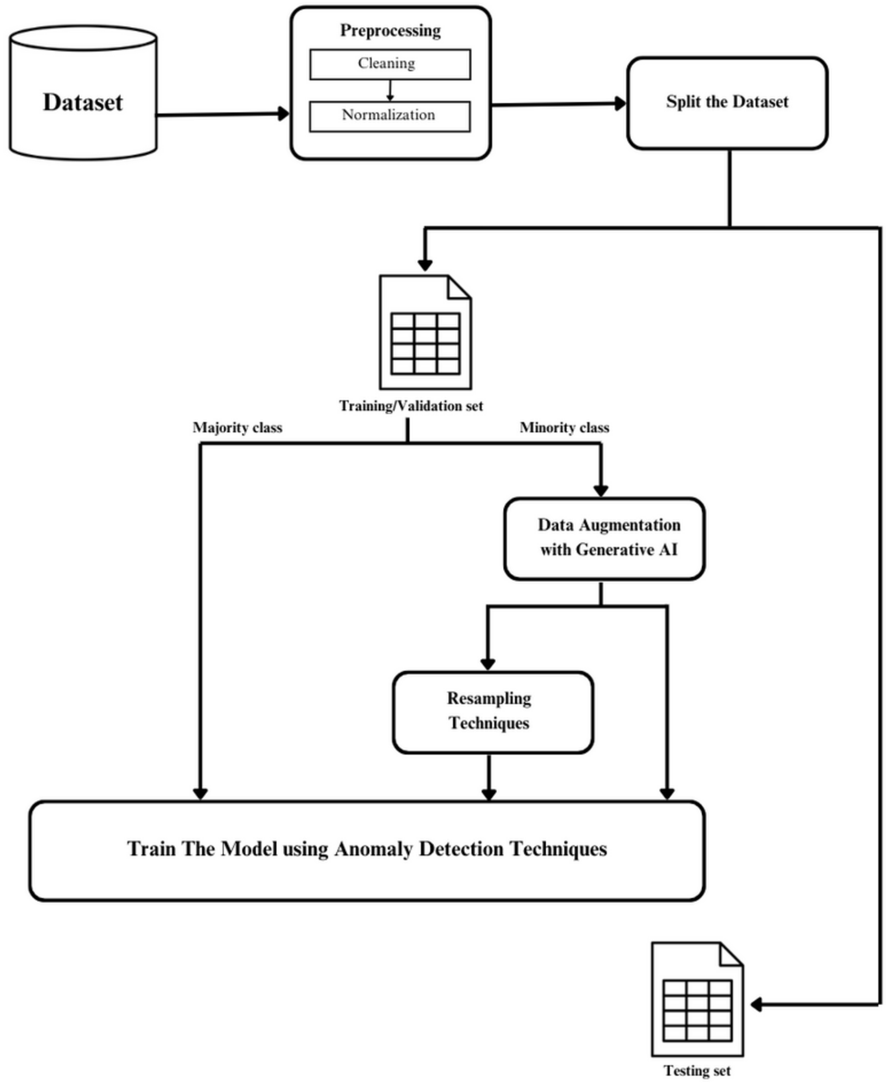
- Selecting a real minority (fraud) sample.
- Finding its nearest neighbors within the fraud class.
- Interpolating between them to create a new, realistic point.



Data Augmentation with Generative AI & SMOTE

Why Combine VAE-GAN + SMOTE ?

- VAE-GAN covers the global patteens.
- SMOTE strengthens local consistency and continuity.
- Together, they create a balanced, diverse, and well structured dataset.



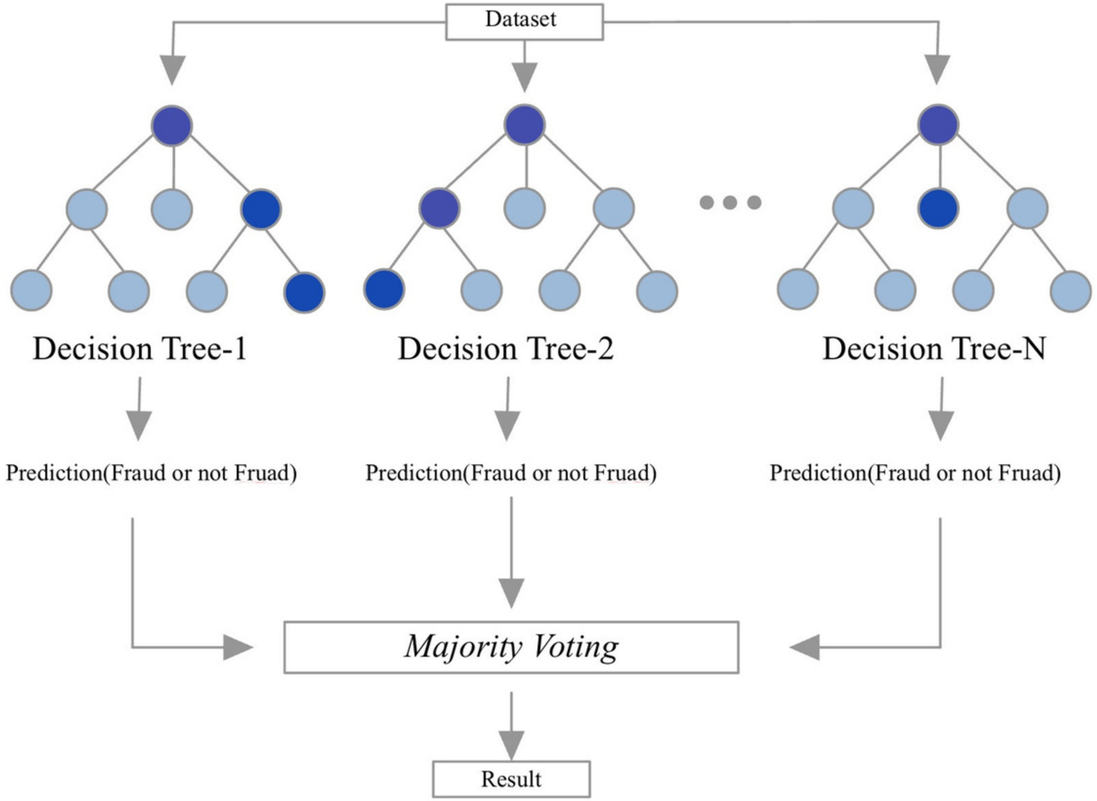
We will compare both approaches:

- VAE-GAN alone
- VAE-GAN + SMOTE

Model Training Using Anomaly detection techniques

Random Forest (Supervised Learning)

- Combines multiple decision trees using majority voting to improve prediction accuracy.
- Trained on labeled data to classify transactions.



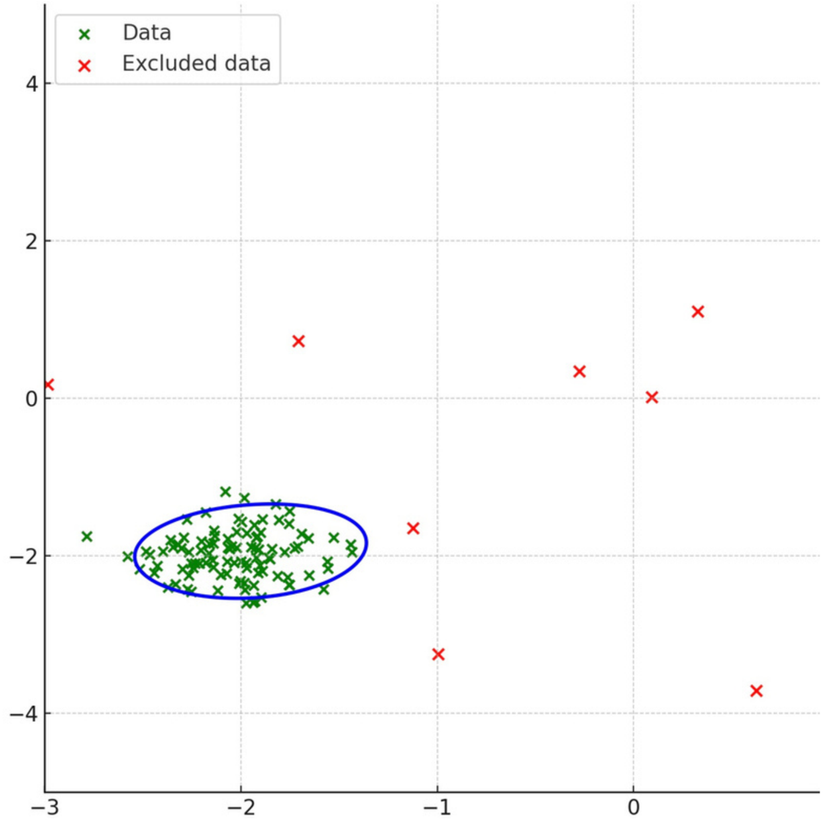
Strengths:

- Handles large, complex datasets.
- Resistant to overfitting.
- Provides high accuracy and interpretability.

Model Training Using Anomaly detection techniques

One-Class SVM (Unsupervised Learning)

- Trained using only the normal data.
- Learns a boundary that encapsulates normal behavior in feature space.



Strengths:

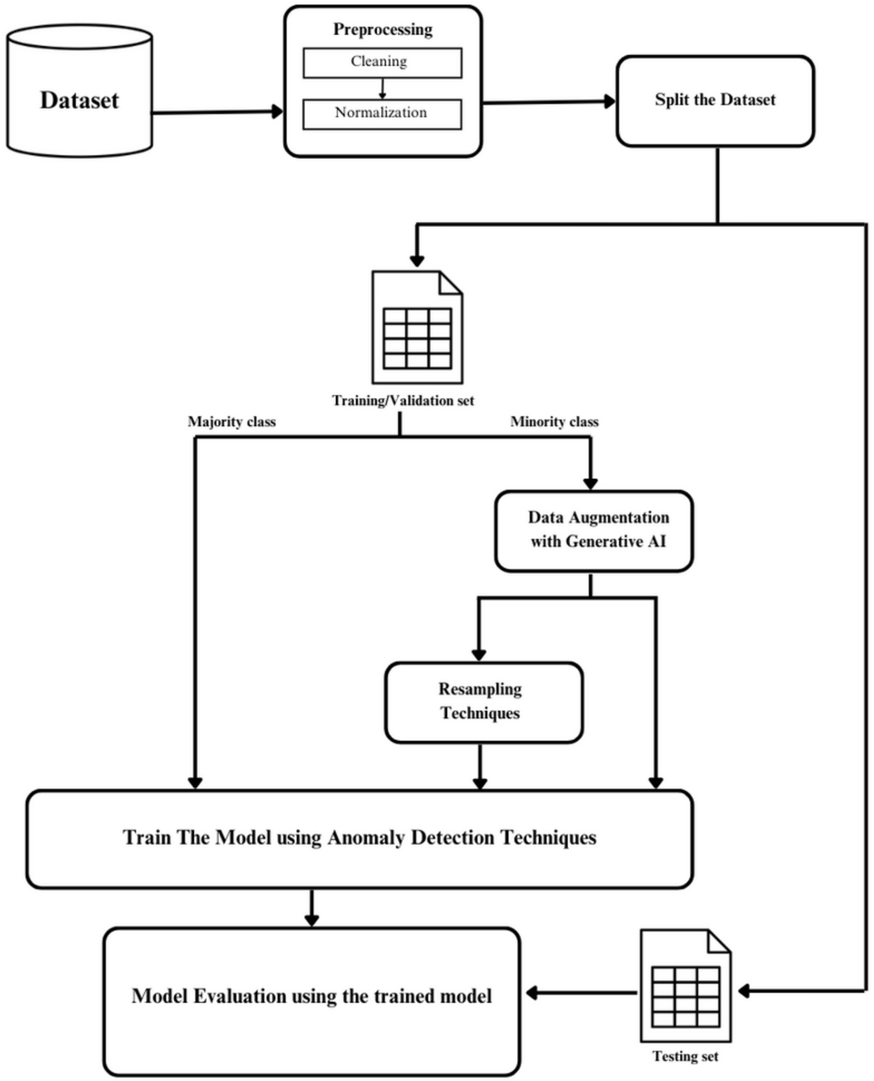
- Useful when fraud labels are scarce or unreliable.
- Detects novel or unexpected fraud patterns.

Both models are trained on the augmented and resampled dataset

Evaluating Model Performance

Evaluation Strategy

- The trained models are assessed using a separate testing set that was not seen during training.
- This ensures a fair and unbiased evaluation of how well the models perform in real-world conditions.



Evaluating Model Performance

- **Evaluation Metrices**

Accuracy

Precision

Recall

F1-Score

Experimental Design

➢ Tools & Libraries

we might use Google Colab as our development environment

Conclusion

AI-BASED FRAUD DETECTION CAN IMPROVE ACCURACY AND EFFICIENCY

MODELS LIKE VAE-GAN HELP CREATE HIGH-QUALITY SYNTHETIC FRAUD SAMPLES.

COMBINING SYNTHETIC DATA WITH CLASSICAL MODELS BOOSTS PERFORMANCE IN IMBALANCED DATASETS.

supports better fraud detection, less loss, more trust.

Thank You.

Any Questions ?