RAKSHNA P

FINAL PROJECT

PROJECT TITLE

CREDIT CARD FRAUD DETECTION IN TRANSACTIONS USING AUTOENCODER

AGENDA

The objective of credit card fraud detection using autoencoder is to identify & prevent fraudulent transactions with in a credit card network . Autoencoders are type of artificial neural network used for unsupervised learning tasks , especially in dimensionality reduction & reconstruction .

PROBLEM STATEMENT

Credit card fraud poses a significant challenge to financial institutions and cardholders alike. With the increasing sophistication of fraudulent techniques, traditional rule-based and statistical methods are often insufficient to detect fraudulent transactions effectively. Therefore, there is a need for advanced techniques that can accurately identify fraudulent activities while minimizing false positives.

PROJECT OVERVIEW

Credit card fraud detection using autoencoder involves leveraging unsupervised learning techniques to identify fraudulent transactions within a credit card network. The process begins with collecting and preprocessing a dataset containing historical credit card transactions. An autoencoder neural network architecture is then developed, comprising an encoder-decoder structure.During the training phase, the autoencoder model learns to reconstruct normal transactions accurately while capturing anomalies indicative of fraudulent behavior.

Training techniques such as mini-batch gradient descent and regularization are applied to optimize the model's performance. Evaluation metrics such as accuracy, precision, recall, and F1-score are used to assess the model's effectiveness.Once trained, the autoencoder model is deployed into the credit card transaction processing system, enabling real-time fraud detection. Integration with existing fraud prevention mechanisms enhances overall security and mitigates financial losses. The expected outcomes include a robust fraud detection system with reduced false positive rates, thereby safeguarding financial assets for both financial institutions and cardholders .

WHO ARE THE END USERS ?

Financial Institutions and Banks: Banks and financial institutions are primary users of credit card fraud detection systems. They utilize autoencoder-based fraud detection to protect their customers' accounts and financial assets from fraudulent activities.

Credit Card Issuers: Companies that issue credit cards, such as Visa, Mastercard, American Express, and various banks, rely on fraud detection systems to safeguard their brand reputation and maintain customer trust.

Cardholders: The end-users of credit cards, i.e., individual consumers and businesses, benefit from fraud detection systems by minimizing the risk of unauthorized transactions and identity theft. Autoencoder-based fraud detection provides cardholders with peace of mind, knowing that their transactions are being monitored for fraudulent activity.

Fraud Investigation Teams: Fraud investigation teams within financial institutions or dedicated security firms use the output of fraud detection systems, including alerts generated by autoencoder models, to conduct further investigation into suspicious transactions.

YOUR SOLUTION AND ITS VALUE PROPOSITION

An autoencoder is a type of artificial neural network used for unsupervised learning, particularly in the field of dimensionality reduction and data compression.

Encoder:

- The encoder takes the input data and maps it to a lower-dimensional latent space representation.

- It consists of one or more layers of neurons that progressively reduce the dimensionality of the input data.

Decoder:

- The decoder takes the compressed representation from the encoder and attempts to reconstruct the original input data.

- It consists of one or more layers of neurons that progressively increase the dimensionality of the latent space representation.

- The final layer of the decoder produces the reconstructed output, which ideally matches the input data.

Training:

- During training, the autoencoder is fed with input data and learns to minimize the difference between the original input and the reconstructed output.

- The loss function measures the discrepancy between the input and the output, such as mean squared error or binary cross-entropy.

- Optimization algorithms like stochastic gradient descent (SGD) or Adam are used to update the parameters of the encoder and decoder to minimize the loss function.

Latent Space Representation:

- The latent space representation learned by the encoder captures the essential features or patterns present in the input data.

- It serves as a compressed and meaningful representation of the input data, facilitating tasks like data visualization, clustering, and anomaly detection.

THE WOW IN YOUR SOLUTION

Self – Representation Learning

Dimensionality Reduction

Feature Extraction

Non Linear Mapping

Unsupervised Learning

Anamoly Detection

Robustness to Noise

Modelling

Python is a widely used programming language in data science and machine learning. Many credit card fraud detection systems are built using Python due to its rich ecosystem of libraries and frameworks. Some of the key libraries for credit card fraud detection in Python include:

Scikit-learn

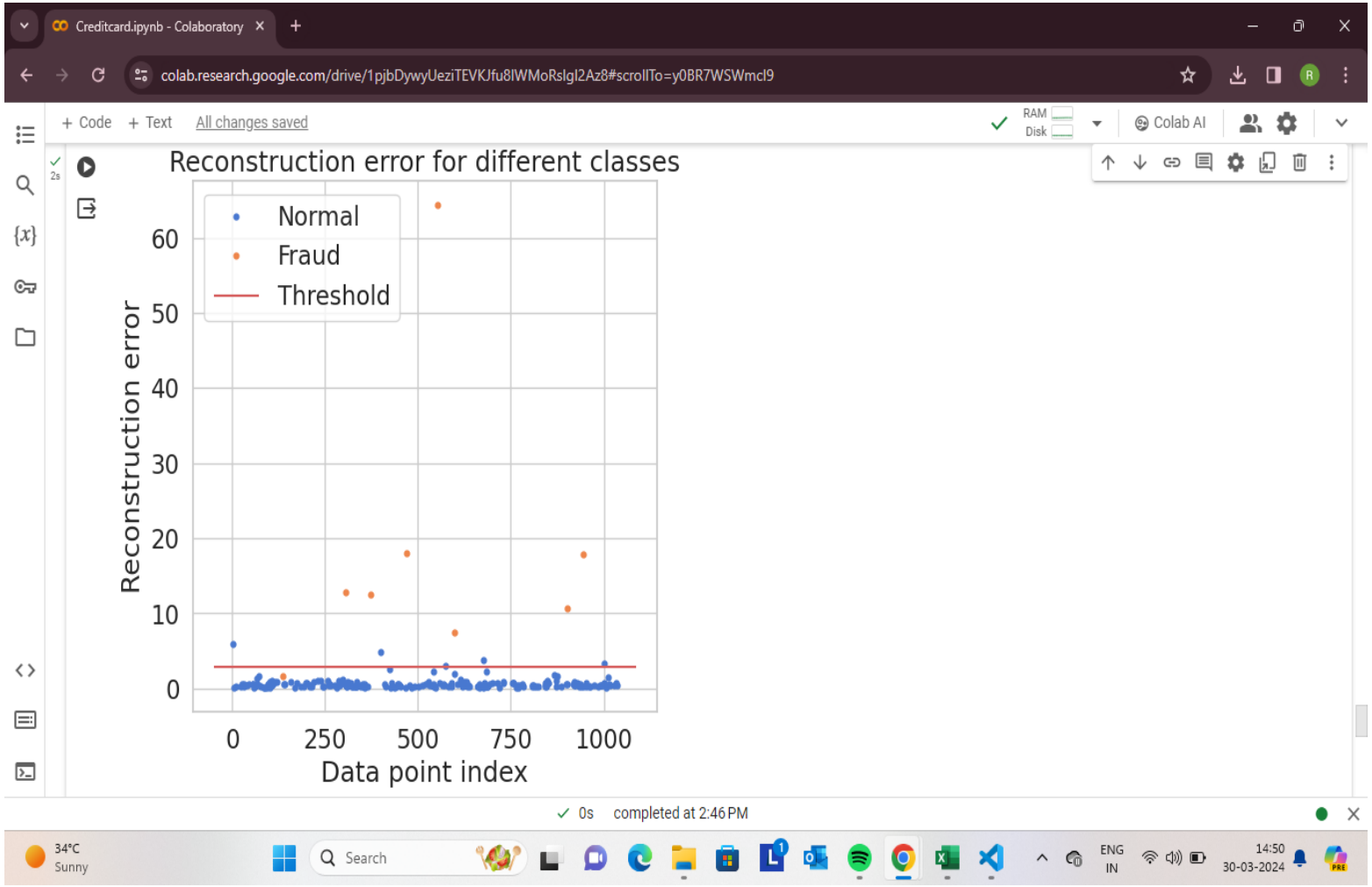
TensorFlow / Keras

PyTorch

Pandas

NumPy

RESULT


Creditcard.ipynb - Colaboratory
colab.research.google.com/drive/1pjbDywyUeziTEVKJfu8IWMoRsIgI2Az8#scrollTo=y0BR7WSWmcI9
+ Code
+ Text
All changes saved
RAM
Disk
Colab AI
Reconstruction error for different classes
Normal
Fraud
Threshold
Reconstruction error
0
10
20
30
40
50
60
0
250
500
750
1000
Data point index
0s
completed at 2:46 PM
34°C
Sunny
Search
ENG
IN
14:50
30-03-2024