PROJECT NAME:

CREDIT CARD FRAUD DETECTION

PROBLEM STATEMENT :

The project aims to develop a machine learning-based system that analyzes transaction data in real-time, effectively detecting credit card fraud while minimizing false positives. This solution will help financial institutions protect against fraudulent transactions, reducing financial losses and ensuring customer trust.

DESIGN THINKING:

- *Data Source: Utilize a dataset containing transaction data, including features such as transaction amount, timestamp, merchant information, and card details.*
- *Data Preprocessing. Clean and preprocess the data, handle missing values, and normalize features.*
- *Feature Engineering. Create additional features that could enhance fraud detection, such as transaction frequency and amount deviations*
- *Model Selection: Choose suitable machine learning algorithms (e.g., Logistic Regression, Random Forest, Gradient Boosting) for fraud detection.*
- *Model Training. Train the selected model using the preprocessed data.*
- *Evaluation: Evaluate the model's performance using metrics like accuracy, precision, recall, F1-score, and ROC-AUC.*

What is credit card fraud?

- *Credit card fraud detection is a set of methods and techniques designed to block fraudulent purchases, both online and in-store.*
- *This is done by ensuring that you are dealing with the right cardholder and that the purchase is legitimate.*

SYNOPSIS :

- *★ Types of credit card frauds*
- *★ Prevention of credit card frauds*
- *★ Detection of credit card frauds*

★*Types of credit card frauds*

- ***Pick pocketing or physical theft:*** *The most obvious way that your credit card could be compromised is through theft. Ensure that your card is always kept safely in your wallet and beware of pickpockets when venturing out. If you're travelling abroad and choose to leave one or more of your cards in your hotel room, make sure they're in a safe or locked up in your suitcase. If your credit card is stolen or lost, make sure you report the theft to your issuer as soon as you become aware of it.*

- ***Skimming card information*** *: A less obvious way that your credit card could be compromised is through skimming. It is the act of stealing the card information rather than the card itself. A card can be skimmed either by swiping it through an illicit card reader or copying out the information manually. To prevent skimming, make sure you do not allow your card to be taken out of your line of sight, and don't swipe it at unverified tellers.*

- ***Carding or cyber-attacks*** *: The most serious and damaging way your card information could be compromised is carding. Here, hackers hack into payment servers and steal thousands of accounts' worth of information. Make it a point to opt for a credit card that takes its security seriously and offers you maximum safety.*

★*Prevention of credit card frauds*

- ***Secure Personal Information*:**
- *->Safeguard your card details, including the card number, expiration date, and CVV code.*
- *->Never share your PIN or passwords with anyone, and choose strong, unique passwords for online accounts.*

- ***Be Cautious with Emails and Calls*:**
- *->Beware of phishing emails or phone calls requesting your card information. Legitimate organizations won't ask for this via email or phone.*
- *->Verify the identity of the caller or sender before sharing any personal information.*

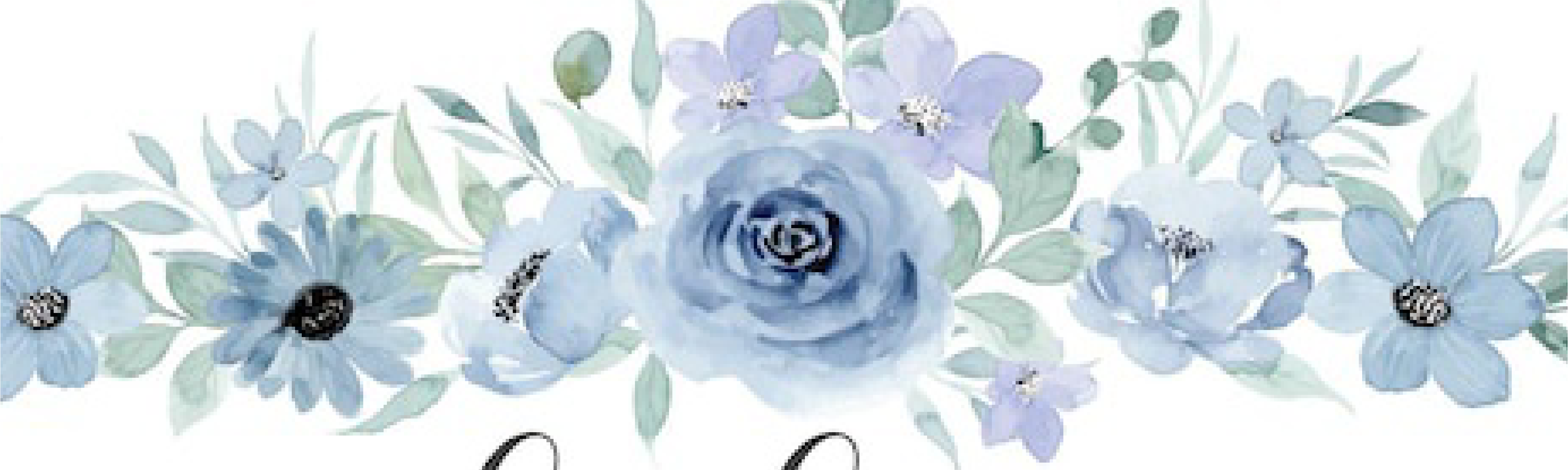
- ***Regularly Monitor Your Accounts:***
- *->Frequently review your credit card statements and transaction history for unauthorized charges.*
- *->Set up account alerts to receive notifications for large or unusual transactions.*

★*Detection of credit card frauds*

- ***Real-time Transaction Monitoring:****Financial institutions and credit card companies employ advanced monitoring systems to analyze every transaction in real-time. These systems automatically flag deviate from the cardholder's typical transactions that appear unusual or spending behavior.*
- ***CVV Verification:****Onlin transactions often require the Card Verification Value (CVV) code on the back of the card to be entered, ensuring that the physical card is in the possession of the user.*

- ***Anomaly Detection***: *Anomaly detection algorithms identify transactions that are significantly different from the norm. Unusual transaction amounts, frequency, or locations can trigger alerts.*
- ***Multi-factor Authentication***:*Multi-factor authentication methods, such as requiring a PIN, biometric data (e.g., fingerprints or facial recognition), or one-time codes, add an extra layer of security during transactions.*
- ***Machine Learning and AI***:*Machine learning models are used to detect patterns of fraudulent activity based on historical transaction data. These models can continuously learn and adapt to evolving fraud tactics.*

- ***Tokenization**: Sensitive card data is replaced with tokens during online transactions, making it difficult for fraudsters to steal valuable information.*
- ***Manual Review** : Some transactions flagged as potentially fraudulent are reviewed by human analysts who can make a final determination.*
- ***Machine Learning Updates** : Models are continuously updated to adapt to new fraud tactics and evolving patterns.*



thank you