1. Problem Statement

Social network platforms are vulnerable to fraudsters who exploit the system to perform malicious activities, such as spamming, phishing, or fake engagements. This project aims to perform an analysis that identifies suspicious behaviour patterns that may indicate fraud by leveraging user data and clustering techniques.

2. Methodology

This project uses the K-Means clustering algorithm, an unsupervised machine learning technique, to identify fraudulent activities in social networks.

Data Collection

- **Dataset Description**: The dataset includes features that reflect user activity, including:
    - **Friends Count**: The number of friends the user has.
    - **Groups Joined**: The number of groups the user is part of.
    - **Posts Per Week**: The number of posts made weekly by the user.
    - **Likes Received**: The total number of likes on the user's posts.
    - **Messages Sent**: The total number of private messages the user has sent.
    - **Login Frequency**: The number of times the user logs in per month.
    - **Time Between Interactions**: The average time gap (in seconds) between consecutive interactions.

Data Preprocessing

- **Standardization**: Since the features (e.g., friend count, likes, and messages sent) have different scales, the data is standardized to have a mean of 0 and a standard deviation of 1 using StandardScaler. This ensures that all features are treated equally during clustering.

Clustering with K-Means

K-Means is chosen for its efficiency in clustering large datasets. The algorithm works by dividing the data points into a predefined number of clusters. The steps we followed include:

- **Elbow Method**: The optimal number of clusters is determined using the Elbow Method, which plots the within-cluster sum of squares (WCSS) for different numbers of clusters.
- **Model Training**: After identifying the optimal number of clusters, K-Means is applied to the dataset. The dataset is clustered based on user behaviours, and each user is assigned to a specific cluster.
- **Cluster Analysis**: Each cluster represents a group of users with similar behaviours. By examining the characteristics of these clusters, suspicious user behaviour is flagged.

For instance, users with very low friend counts but high message activity could potentially indicate fraudulent behaviour.

Fraud Detection

To identify fraudulent users:

- **Cluster Centers**: The cluster centers, which represent the average behaviour of users in each cluster, are analysed to identify abnormal patterns.
- **Outlier Detection**: Outliers in the clusters that exhibit suspicious behaviour patterns (e.g., high activity but low friends or group membership) are flagged for further investigation.

3. Tools and Technologies Used

- **Python**: The project is implemented in Python, leveraging several libraries for data manipulation, clustering, and visualization.
  - **Pandas**: For managing the dataset and performing data preprocessing.
  - **NumPy**: For numerical operations.
  - **Scikit-learn**: For applying the K-Means clustering algorithm and standardizing the data.
  - **Matplotlib & Seaborn**: For data visualization, including the elbow plot and cluster analysis.
- **Google Colab**: The entire project was executed on Google Colab, which provides an efficient environment for running Python code and training machine learning models. Colab is ideal for this task due to its built-in support for common Python libraries and its ability to handle large datasets.

4. Results and Discussion

- **Cluster Analysis**: The clustering results divided the users into three groups, each representing different behaviour patterns, namely cluster with high engagement, cluster with moderate engagement and cluster with potential fraud.
- **Fraud Detection**: Based on the clustering results, a group of users was identified as suspicious. These users have low social engagement but high activity in terms of posts and messages. Such users could potentially be fraudsters exploiting the platform for spamming or other malicious activities.

5. Conclusion

Fraud detection using clustering techniques provides a robust method for identifying abnormal behaviour in social networks. By analysing user activity patterns and clustering them into groups, we can flag potential fraudulent behaviour. The unsupervised K-Means clustering algorithm allows for fraud detection without the need for labeled data, making it ideal for exploratory analysis.