PROBLEM STATEMENT :

***There are social engineering frauds in which fake accounts of prominent people are created on social media and their friends are approached to transfer certain money into the accounts of fraudsters. Give a technical solution to be adopted by social media firms in which such types of fraud accounts are automatically deleted.***

#### **1. Project Overview:**

The objective of this project is to develop a technical solution to detect and automatically delete fraudulent accounts on social media platforms that are used for social engineering scams. These scams typically involve creating fake accounts of prominent individuals and soliciting money from their friends or followers. Our solution will use AI-based tools to verify account authenticity, monitor interactions for suspicious behavior, and prevent fraudulent actions before they escalate.

#### **2. Solution Approach:**

Our approach involves several key components:

* **Profile Verification:** Ensuring account authenticity using AI and facial recognition.
* **Behavioral Analysis:** Monitoring unusual interaction patterns that indicate fraudulent activity.
* **Message and Transaction Filtering:** Analyzing communications for financial fraud indicators.
* **Automated Deletion:** Implementing an automated system for deleting or flagging fake accounts after detecting suspicious activities.

#### **3. Technical Framework:**

* **1. Profile Verification:**
  + **Facial Recognition:** Compare profile images against known databases to identify fake photos or stock images. Use tools like Google Vision or OpenCV for image verification.
  + **Metadata Analysis:** Track account creation date, activity frequency, and profile completeness to detect anomalies.
* **2. Behavioral Analysis:**
  + **Interaction Patterns:** Track patterns in friend requests, messaging, and post engagements to identify coordinated activity (e.g., large numbers of new accounts connecting with a prominent person).
  + **Machine Learning Algorithms:** Train models to detect behavior that deviates from normal user interactions. The model would flag suspicious accounts for review.
* **3. Message Filtering:**
  + **Natural Language Processing (NLP):** Analyze messages for keywords and patterns indicative of social engineering tactics (e.g., emergency, money transfer requests).
* **4. Fraud Detection and Blocking:**
  + **Anomaly Detection System:** Build a system to automatically flag accounts with unusual behaviors, blocking them temporarily for further review.
  + **Threshold Alerts:** Accounts reaching predefined thresholds of suspicious behavior (e.g., rapid friend requests, sudden financial messaging) will be flagged for deletion.
* **5. Automation and Reporting:**
  + **Automated Deletion:** Once an account is flagged, it will be deleted or blocked after a certain period for review.
  + **User Reporting Integration:** Enable users to report suspicious accounts, feeding into the algorithm to improve fraud detection.

#### **4. Anticipated Outcomes:**

* **Fewer Fraudulent Accounts:** A reduction in the number of fake accounts being used for scams, improving user safety.
* **Automated Fraud Detection:** The system will automatically flag and delete fraudulent accounts based on pre-set thresholds, reducing the need for manual intervention.
* **Improved User Trust:** Users will feel more secure knowing that the platform actively prevents fraud and protects personal data.
* **Scalable Solution:** The framework can be scaled to accommodate a growing user base and continuously improve fraud detection techniques.

#### **5. Technical Tools and Resources:**

* **AI Tools:** OpenCV, TensorFlow (for facial recognition and behavioral analysis)
* **Natural Language Processing:** NLTK, spaCy (for message filtering)
* **Backend Infrastructure:** Node.js, Python (for building APIs and processing data)
* **Cloud Storage:** AWS, Google Cloud (for storing user data securely)
* **Database:** MySQL, MongoDB (for storing account and interaction data)

**6. Conclusion:**

This project provides an innovative solution to combat social engineering fraud on social media platforms by leveraging modern AI techniques. The automated approach to detecting fraudulent accounts ensures that users are protected, and the platform maintains a high level of integrity. By implementing this system, social media firms can effectively prevent financial scams and improve user trust.