***AI-Driven Entity Risk Analysis: Architecture & Design***

# Overview

The **AI-driven Entity Risk Analysis** system is designed to analyze and calculate the risk levels associated with entities based on multiple real-time public data sources (APIs). It uses advanced AI techniques, including **Natural Language Processing (NLP)** and **Sentiment Analysis**, to dynamically evaluate risk based on structured (CSV) and unstructured (text) inputs. The system is integrated with multiple public APIs, such as **OFAC**, **OpenSanctions**, **News**, **Wikidata**, and others, to gather entity data and assess its risk.

This document outlines the **solution architecture** and design of the system, focusing on how the **APIs** and **AI** are used in the risk analysis process, in line with the problem statement.

# Solution Architecture

The **architecture** consists of multiple layers that work together to fetch data, process it, and generate insights. These include:

1. **Input Layer**:
   * **Structured Data**: CSV files containing transaction data.
   * **Unstructured Data**: Text files containing transaction data with various entities.
2. **Entity Extraction Layer**:
   * **Entity Extractor**: This module uses **regular expressions** and **AI-based named entity recognition (NER)** to extract relevant entities like sender, receiver, approver, intermediary, etc., from both structured and unstructured data.
3. **API Integration Layer**:
   * The system integrates with several public APIs to gather real-time data and evaluate the risk associated with the extracted entities. Key APIs include:
     + **OFAC Sanctions List**: Checks if the entity is listed in the **OFAC SDN List**.
     + **OpenSanctions**: Gathers data about entities from **sanctions lists**, such as PEP (Politically Exposed Persons).
     + **News API**: Uses news data to perform **sentiment analysis** on the entity’s reputation.
     + **Wikidata**: Fetches general information about the entity, such as description and associated tags.
     + **Clearbit**: Provides company-related data (e.g., logo, company information).
     + **Wayback Machine (archive.org)**: Checks historical records for the entity’s website.
     + **DuckDuckGo Instant Answer**: Provides brief summaries and additional metadata about entities.
4. **Risk Scoring and Sentiment Analysis Layer**:
   * **Risk Scoring**: The system calculates a **risk score** based on the presence of the entity in different sources and its **sentiment score**.
   * **Sentiment Analysis**: **Sentiment polarity** from news data is used to modify the risk score. If the sentiment is negative, the entity’s risk score is increased.
   * **Confidence Score**: The confidence score reflects the amount of real data available to assess the entity. It is based on how many sources were found for the entity, with a maximum cap of 1.0.
5. **Reason Generation Layer**:
   * After gathering data from the APIs, the system generates a **reason** for the risk score based on the entity’s profile. This reason is human-readable and explains why the entity was flagged with a specific risk score.
   * The reason takes into account data from different sources, such as **sanctions lists**, **sentiment analysis**, and **news articles**.
6. **Output Layer**:
   * **Final Output**: The output consists of a **JSON file** with the following fields for each transaction:
     + **Extracted Entity**: List of entities (e.g., company names).
     + **Entity Type**: Classification of the entity (e.g., Corporation, Individual).
     + **Risk Score**: A numerical score representing the entity’s risk level (0.0 to 1.0).
     + **Confidence Score**: The confidence in the accuracy of the risk score.
     + **Supporting Evidence**: List of sources that contributed to the entity’s risk score.
     + **Reason**: A human-readable explanation of why the entity was flagged with that particular score, including detailed information about the entity’s presence in different risk-related sources.

# How APIs and AI are Integrated into the Process

1. **API Calls**: For each entity extracted from the transaction data, the system makes calls to the APIs:
   * **OFAC**: Checks the entity against the **OFAC SDN List**.
   * **OpenSanctions**: Fetches information on whether the entity is on any sanctions list or involved in illegal activities.
   * **News API**: Sentiment analysis is performed on news articles associated with the entity. If the sentiment is negative, it increases the risk score.
   * **Wikidata**: The description and classification of the entity are used for contextual information, enhancing the risk scoring.
   * **Clearbit, Wayback, DuckDuckGo**: Fetch additional metadata to validate the entity’s profile and reputation.
2. **AI Models**:
   * **Risk Calculation**: The AI model calculates risk scores based on the data returned from the APIs. The **sentiment score** from the News API is factored into the risk calculation to adjust the final score.
   * **Reasoning**: An AI-driven reasoning engine is used to generate a human-readable summary of why the entity has been flagged with a specific risk score.
3. **Score and Reasoning Calculation**:
   * Each **API source** contributes a weight to the final risk score based on its relevance.
   * The **sentiment score** modifies the risk score based on the **sentiment of the news articles**.
   * A **confidence score** is calculated based on how many valid data points (i.e., sources) are available for the entity.

# Architectural Flow

The architectural flow can be described as follows:

1. **Data Input**: Structured (CSV) and unstructured (text) data are provided as input.
2. **Entity Extraction**: Named entities such as company names and individuals are extracted from both structured and unstructured data.
3. **API Integration**: API calls are made to gather information about each extracted entity.
4. **Risk Scoring**: Risk scores are dynamically calculated based on the information fetched from the APIs, taking into account the sentiment of news articles and the presence of the entity in sanctions lists.
5. **Reason Generation**: The reason for each entity’s risk score is generated in a human-readable format, explaining why the entity is flagged as high or low risk.
6. **Output**: The final result is saved in a **JSON file**, which includes the extracted entities, risk scores, confidence scores, supporting evidence, and reasons.

# Key Highlights

* **Dynamic Risk Scoring**: The risk score is calculated dynamically based on real-time data fetched from public APIs. The score adjusts according to sentiment, presence in risk lists (OFAC, OpenSanctions), and other metadata.
* **Human-Readable Reasoning**: The reason field is not a raw output from the APIs but is a human-readable explanation of why the entity is flagged with a particular risk score. The reasoning is derived from the data obtained from the APIs.
* **Confidence Scoring**: Confidence in the final risk score is based on how many valid data sources (e.g., API results) contribute to the decision.
* **AI Integration**: AI is used to process sentiment analysis, generate dynamic reasons, and calculate risk based on multiple data sources.

# Conclusion

This solution provides a robust framework for risk analysis, leveraging both **AI** and **real-time data from public APIs**. By dynamically calculating risk based on the presence of entities in multiple sources, including sanctions lists and sentiment from news, the system offers a transparent and explainable method for assessing entity risk.

Let me know if you need further clarifications or adjustments!