Project Title: Hidden Markov Model for Credit Fraud Detection
Group Number: [Insert Group Number]
URL of Project's Website: [Insert URL]

Team Profile
Team Members:
1. [Member 1 Name] - [Qualifications and Strengths] (e.g., programming, design, statistical analysis)
2. Joseph Judkins - [Learning skills, problem-solving skills, programming skills, proficient in Python]

Note: It is expected that every team member shall be involved in all project activities; this only indicates individual strengths, not their sole responsibilities.

Team Leader: [Name of the elected team leader] (if applicable)

Proposed Project Description

1. Introduction
Credit fraud is a significant and growing issue that impacts individuals and organizations globally. Current systems often struggle to keep up with sophisticated fraudulent activities due to their rigidity and potential inability to detect subtle, evolving patterns of fraud. This project proposes to develop a system using Hidden Markov Models (HMM) to effectively detect credit fraud in transactions. Hidden Markov Models offer a probabilistic framework, possibly capturing temporal patterns in sequential data. This makes it well suited for detecting anomalies in credit card transaction sequences. HMMs can identify deviations by modeling a customer's typical transaction behavior, which can indicate fraud and other similar fraudulent activities.

2. Problem Diagnosis
The problem domain involves detecting fraudulent transactions in credit systems. The issues with current practices include:
- **High False Positive Rates:** Existing systems frequently flag legitimate transactions as suspicious because they rely on generalized rules. This is an issue because some customers have erratic behavior, but they are legitimate purchases. False positives result in frustration for customers, especially those whose accounts are frozen unnecessarily, and create burdens for companies or other institutions that must handle increased volumes of fraud investigations.
- **Inability to Adapt:** Fraudulent schemes are often evolving, with fraudsters constantly innovating ways to scam their victims. Rule based systems struggle to keep pace with them, struggling to adapt and often requiring manual updates. These updates then become more reactionary instead of proactive, which does not help the person who was scammed. These systems lack flexibility to adapt dynamically. This makes them more ineffective when it comes to detecting new behaviors or tactics as patterns evolve further.

- **Data Volume:** Monetary transactions are the backbone of society, with millions of people making multiple transactions each day. Keeping track of all of them to detect fraud is no small feat. With online banking and e-commerce, these transactions are more virtual than ever, making detection of real-time fraud a massive challenge. Conventional systems can struggle to process this much information at once, and struggle to detect fraud quickly enough to catch fraudsters in the act. This results in delayed responses. With all data needing to be analyzed in real time, the traditional methods can sometimes struggle to keep up with the sheer demand and number of transactions.

*Example scenarios of these issues might include interviews with financial institutions that discuss their current challenges with fraud detection, with those issues being false positives. A global bank might report that while its current fraud detection system effectively blocks fraudulent transactions, the system may also frequently flags legitimate purchases, with this problem being especially prevalent during days like Black Friday, something similar may occur in the case of international travel. The detection system may determine that a purchase was made in another country, and flag it without determining whether the user is in that country on vacation or not. Financial institutions also may express concerns about adaptability, with manual updates being more reactionary than proactive, as it can be hard to guess what a fraudster will do before they do it. In these scenarios, reactionary combat of fraud may not help the people who are first affected by these fraudulent actions. *

3. Proposed Treatment
To address the diagnosed problems, we propose the following interventions:
- **Implementation of HMM** that models the sequence of transactions to identify unusual patterns indicative of fraud. By identifying the underlying hidden states, be it legitimate or fraudulent, the model will flag transactions that deviate from the usual patterns. This approach addresses limitations of static, rule based systems by continuously learning and adapting to fraud tactics. Additionally, the probabilistic nature of HMM can allow it to detect subtle shifts in behavior that may signal fraud, reducing the chance of false positives and improving accuracy.
- **Real-time Monitoring** to analyze transactions as they occur and flag suspicious ones for further review. This is done to make sure that everything is done in a timely manner. The system will calculate the probability of each transaction being legitimate, and flag transactions that fall out of the normal range of expected behavior. This allows for immediate intervention, such as flagging the transaction for review or temporarily freezing the account to prevent further unauthorized transactions. The real-time monitoring will address the issue of delayed detection in high-volume transaction environments, which ensures faster responses to potential frauds.
- **User-Friendly Dashboard** for analysts to view flagged transactions and insights. This dashboard will display key metrics such as transaction sequence, probability scores, and contextual information, such as location, time, and behavior history. Analysts can then use this tool to review flagged transactions more effectively, providing them with necessary information to make informed decisions. Streamlining this process through the dashboard will help reduce manual effort, improve fraud investigation efficiency, and minimize disruptions to legitimate users.

Metrics for success will include reduced false positives, increased detection rates, and improved analyst response times. If we consider a user who regularly makes small transactions in their local area, but then makes a large one in an international location, the HMM will analyze the sequence of recent transactions. If there is a large deviation from typical behavior, the model will assign a low probability to the legitimacy of the transaction. It will then flag the transaction for further review by an analyst via the dashboard. The analyst, armed with detailed insights and transaction history, can then quickly assess the risk and take the needed actions, such as contacting the customer or freezing the account.

Plan of Work

1. Initial Steps (Next Few Weeks):
- Research existing HMM algorithms and their application to fraud detection.
- Gather requirements from potential users in the financial sector to tailor the solution to real needs.

2. Functional Features:
- **Transaction Analysis:** Detect patterns in transaction sequences.
- **Alerts Generation:** Notify users of flagged transactions based on predefined thresholds.
- **Reporting Tools:** Generate reports showing detection rates, false positives, and other relevant metrics.

Each team member will be responsible for specific functionalities, such as:
- [Member 1 Name]: Development of the transaction analysis module.
- [Member 2 Name]: Implementation of the alerts generation mechanism.

3. Product Ownership:
Each team member's contributions will be clearly defined to ensure accountability, with an emphasis on functional feature ownership rather than subsystems.

Conclusion
This proposal aims to leverage the HMM to provide a robust solution to credit fraud detection. By thoroughly diagnosing the problem, prescribing a targeted treatment, and outlining a clear plan of work, we aim to create a beneficial system for financial institutions.

Important Considerations:
- Confirm the availability of datasets required for model training and validation.
- Outline any additional resources or expertise needed (e.g., access to financial transaction data, knowledge in data security).
