


## Ideation Phase

### Brainstorm & Idea Prioritization

Date	18 October 2023
Team ID	593197
Project Name	PayGuard Plus – An Online Payments Fraud Detector
Maximum Marks	4 Marks
Team Size	3
Member 1 – Team Lead	Akshit Bahl (21BIT0012)
Member 2	Ananya Priya (21BIT0245)
Member 3	Lakshya Mittal (21BIT0076)

### Brainstorm & Idea Prioritization Template:

#### Step-1: Team Gathering, Collaboration and Select the Problem Statement



### Brainstorm & idea prioritization

**PayGuard Plus:**

An efficient solution to all your online payments fraud problems.

🕒 10 minutes to prepare  
🕒 1 hour to collaborate  
👤 2-8 people recommended

---

**Team Members:**

1. Akshit Bahl
2. Ananya Priya
3. Lakshya Mittal

**Before you collaborate**

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

🕒 10 minutes

---

- A Team gathering**  
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.
- B Set the goal**  
Think about the problem you'll be focusing on solving in the brainstorming session.
- C Learn how to use the facilitation tools**  
Use the Facilitation Superpowers to run a happy and productive session.

[Open article](#) →


**1 Define your problem statement**

In an increasingly digital and interconnected world, online payment fraud poses a significant threat to both businesses and consumers. The objective of this project is to develop a comprehensive and efficient Online Payment Fraud Detection System using machine learning algorithms. The system's primary goal is to safeguard financial transactions, protect businesses from financial losses, and ensure the security and trust of online payment platforms.

**PROBLEM 1**

**How might we ?**

How might we develop an efficient online payment fraud detection system that protects businesses and consumers from financial fraud while minimizing inconvenience to legitimate users and ensuring compliance with data protection regulations?



**Key rules of brainstorming**

To run a smooth and productive session

👤 Stay in topic.

💡 Encourage wild ideas.

👂 Defer judgment.

👂 Listen to others.

🗣️ Go for volume.

👁️ If possible, be visual.

## Step-2: Brainstorm, Idea Listing

2

### Brainstorm

Write down any Ideas that come to mind that address your problem statement.

🕒 10 minutes

#### TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

#### Akshit Bahl

Gather a diverse and extensive dataset of online payment transactions, including both legitimate and fraudulent ones.

Use techniques like one-hot encoding, scaling, and aggregation to preprocess the data.

Utilize feature selection methods to identify the most relevant features for fraud detection, improving model efficiency.

Develop a system that can monitor online payment transactions in real-time.

Implement a feedback loop that continuously learns from new data and adapts the model to emerging fraud patterns.

Use geolocation data to verify the user's physical location and detect transactions originating from unexpected locations.

#### Ananya Priya

Collect additional data, such as user profiles, device information, and transaction history.

Choose appropriate machine learning algorithms, such as logistic regression, decision trees, random forests, support vector machines, or neural networks.

Experiment with various hyperparameters and model architectures to find the best-performing solution.

Implement a scoring system to assign risk scores to each transaction.

Incorporate multi-factor authentication to enhance user security and reduce the risk of fraud.

Ensure that the system can provide explanations for its decisions, which can be crucial for fraud investigation and compliance purposes.

#### Lakshya Mittal

Create meaningful features from the raw data, including transaction amount, location, time of day, user behavior, and more.

Experiment with ensemble methods to combine the strengths of multiple algorithms.

Address class imbalance by using techniques like oversampling, undersampling, or Synthetic Minority Over-sampling Technique (SMOTE).

Set thresholds for risk scores to decide when a transaction should be flagged for further review.

Analyze user behavior patterns to identify deviations that might signal fraudulent activity.

Deploy the fraud detection model as a real-time API or integrate it into existing payment processing systems.

## Step-3: Grouping

3

### Group Ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you can break it up into smaller sub-groups.

🕒 20 minutes

#### TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.

### Data Collection

The project aims to collect a diverse and extensive dataset of online payment transactions. This dataset should encompass both legitimate and fraudulent transactions. Additionally, data such as user profiles, device information, and transaction history will be gathered to enhance the detection capabilities of the system.

### Feature Engineering

The system will create meaningful features from the raw data. These features will include transaction amount, location, time of day, user behavior, and more. Techniques like one-hot encoding, scaling, and aggregation will be employed to preprocess the data effectively.

### Algorithm Selection

The project will choose suitable machine learning algorithms, such as logistic regression, decision trees, random forests, support vector machines, or neural networks. Ensemble methods will be explored to combine the strengths of multiple algorithms.

### Model Training and Validation

The data will be split into training, validation, and testing sets. Various hyperparameters and model architectures will be experimented with to find the best-performing solution.

### Real-Time Monitoring

The system will be designed to monitor online payment transactions in real-time. It will implement a scoring system to assign risk scores to each transaction. Appropriate thresholds will be set for risk scores to decide when a transaction should be flagged for further review.

### Compliance & Integration

The system will adhere to data protection and privacy regulations, such as GDPR or CCPA, to ensure the security and privacy of user data. The fraud detection system will seamlessly integrate with various payment gateways and e-commerce platforms to provide a cohesive and secure payment experience.

### Monitoring and Alerts

The project will implement a system that sends alerts and notifications to administrators or users when potential fraud is detected.

## Step-4: Prioritize Ideas based on Importance and Feasibility

4

### Prioritize

Your team should all be on the same page about what's Important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

🕒 20 minutes

#### TIP

Participants can use their cursors to point at where sticky notes should go on the grid. The facilitator can confirm the spot by using the laser pointer holding the H key on the keyboard.

