

IdeationPhase


Brainstorm & Idea Prioritization

Date	07October2023
TeamID	NM2023TMID09503
ProjectName	Biometric Security System For Voting Platform
MaximumMarks	4Marks

Brainstorm & Idea Prioritization:

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


Template



Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

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



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

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

🕒 5 minutes

PROBLEM

Biometric data is unique to each individual, making it difficult for anyone to fraudulently cast multiple votes or impersonate others. This strengthens the integrity of elections by minimizing voter fraud. Ensuring the security of voting machines, electronic voting systems, and online voting platforms is vital.



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 and Grouping

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!

SRISABARI

Implement a multi-modal biometric system that combines multiple biometric identifiers, such as fingerprints, iris scans, and facial recognition. This increases the accuracy of identity verification and makes it more difficult for fraudulent attempts.

SHARUKESHAN

Utilize blockchain technology to create a secure and transparent ledger of votes. Each vote is encrypted and added to the blockchain, making it tamper-proof and easily auditable.

VEDANAYAGAM

Use biometric data during voter registration to ensure that each voter's identity is accurately verified. This can be done during the initial registration process to create a secure database of eligible voters.

SRUTHIE

Encrypt and protect biometric data using state-of-the-art encryption techniques to prevent unauthorized access or data breaches. Data should only be accessible for authentication purposes.

Implement anti-spoofing measures to detect and prevent attempts to use fake or replicated biometric data for authentication.

Ensure the system is accessible to all voters, including those with disabilities. Provide options for voice commands, braille display, or other accessibility features to ensure inclusivity.

Develop a system that ensures the anonymity of voters. Votes are tied to biometric data for authentication but separated from personal information to protect privacy.

Create a hybrid voting system that combines traditional paper ballots with biometric authentication. Voters can choose their preferred method while still benefiting from biometric security.

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 and 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 they show within your mind.

Collaborate with national ID systems to streamline the voter registration process, using biometric data already collected for other purposes, such as ID cards or passports. These ideas can be integrated into a comprehensive Biometric Security System for a Voting Platform to enhance security, transparency, and accessibility in the electoral process. The specific features and technologies used should align with the legal and regulatory requirements of the region in which the system is deployed.

Establish clear and strict policies for the retention and deletion of biometric data to address privacy concerns and data protection regulations.

Step-3:IdeaPrioritization

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.

Importance

If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?

Implement a multi-modal biometric system that combines multiple biometric identifiers, such as fingerprints, iris scans, and facial recognition. This increases the accuracy of identity verification and makes it more difficult for fraudulent attempts.

Encrypt and protect biometric data using state-of-the-art encryption techniques to prevent unauthorized access or data breaches. Data should only be accessible for authentication purposes.

Create a hybrid voting system that combines traditional paper ballots with biometric authentication. Voters can choose their preferred method while still benefiting from biometric security.

Utilize blockchain technology to create a secure and transparent ledger of votes. Each vote is encrypted and added to the blockchain, making it tamper-proof and easily auditable.

Implement anti-spoofing measures to detect and prevent attempts to use fake or replicated biometric data for authentication.

Establish clear and strict policies for the retention and deletion of biometric data to address privacy concerns and data protection regulations.

2