**Ideation Phase**

**Brainstorm & Idea Prioritization Template**

|  |  |
| --- | --- |
| Date | 19 September 2022 |
| Team ID | PNT2022TMID593505 |
| Project Name | AI System That Verifies User Identities Based On Their Online Behavior Patterns, Adding An Extra Layer Of Security |
| Maximum Marks | 4 Marks |

**Brainstorm & Idea Prioritization Template:**

Brainstorming provides a free and open environment that encourages everyone within a team to participate in the creative thinking process that leads to problem solving. Prioritizing volume over value, out-of-the-box ideas are welcome and built upon, and all participants are encouraged to collaborate, helping each other develop a rich amount of creative solutions.

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.

Reference: <https://www.mural.co/templates/empathy-map-canvas>

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

Graphical user interface, application

Description automatically generated

**Step-2: Brainstorm, Idea Listing and Grouping**

Graphical user interface, treemap chart

Description automatically generated

**Step-3: Idea Prioritization**

**Diagram

Description automatically generated**

Step 1:

Problem statement:

AI systems that verify user identities based on their online behavior patterns can provide an extra layer of security, but they also raise concerns about privacy, security, and reduced control.

Privacy concerns:

* AI systems that track online behavior patterns can collect a vast amount of data about users, including their browsing history, search queries, social media activity, and purchase history. This data can be used to create detailed profiles of users, which could be used for targeted advertising, surveillance, or other purposes without the user's knowledge or consent.
* AI systems can also be used to identify and track individuals even if they are using anonymous or pseudonymous accounts. This could be used to track people's movements, monitor their activities, or even blackmail them.

Security fears:

* AI systems that verify user identities based on online behavior patterns can be vulnerable to attack. For example, attackers could create fake data or manipulate existing data to fool the AI system into thinking that they are legitimate users. This could allow attackers to gain unauthorized access to accounts or systems.
* AI systems can also be biased, which could lead to false positives and false negatives. For example, an AI system that is trained on data from a predominantly white population may be less accurate at identifying and verifying users from other racial or ethnic groups.

Reduced control:

* AI systems that verify user identities based on online behavior patterns can reduce users' control over their own data and their digital identities. For example, if an AI system decides that a user is not behaving in a "normal" way, it could block the user from accessing their account or system. This could have negative consequences for the user's personal life or professional life.

Step 2:

Solutions:

* Transparency: AI systems that verify user identities based on online behavior patterns should be transparent about how they work and what data they collect. Users should be able to understand how their data is being used and how it is being protected.
* Choice: Users should have the choice of whether or not to use AI systems to verify their identities. They should also have the choice of whether or not to share their data with AI systems.
* Control: Users should be able to control how their data is used by AI systems. They should be able to opt out of having their data used for AI-powered identity verification, and they should be able to delete their data from AI systems.
* Accountability: AI systems that verify user identities based on online behavior patterns should be accountable to users and to the public. There should be mechanisms in place to ensure that AI systems are used fairly, ethically, and responsibly.

Step 3:

Here is a prioritized list of the solutions:

* Transparency: Transparency is the most important factor in our opinion because it allows users to make informed decisions about whether or not to use AI-powered identity verification systems and how to share their data with these systems.
* Choice: Choice is the second most important factor in our opinion because it gives users control over their own data and their digital identities.
* Control: Control is the third most important factor in our opinion because it allows users to limit how their data is used by AI-powered identity verification systems.
* Accountability: Accountability is the fourth most important factor in our opinion because it helps to ensure that AI-powered identity verification systems are used fairly, ethically, and responsibly.