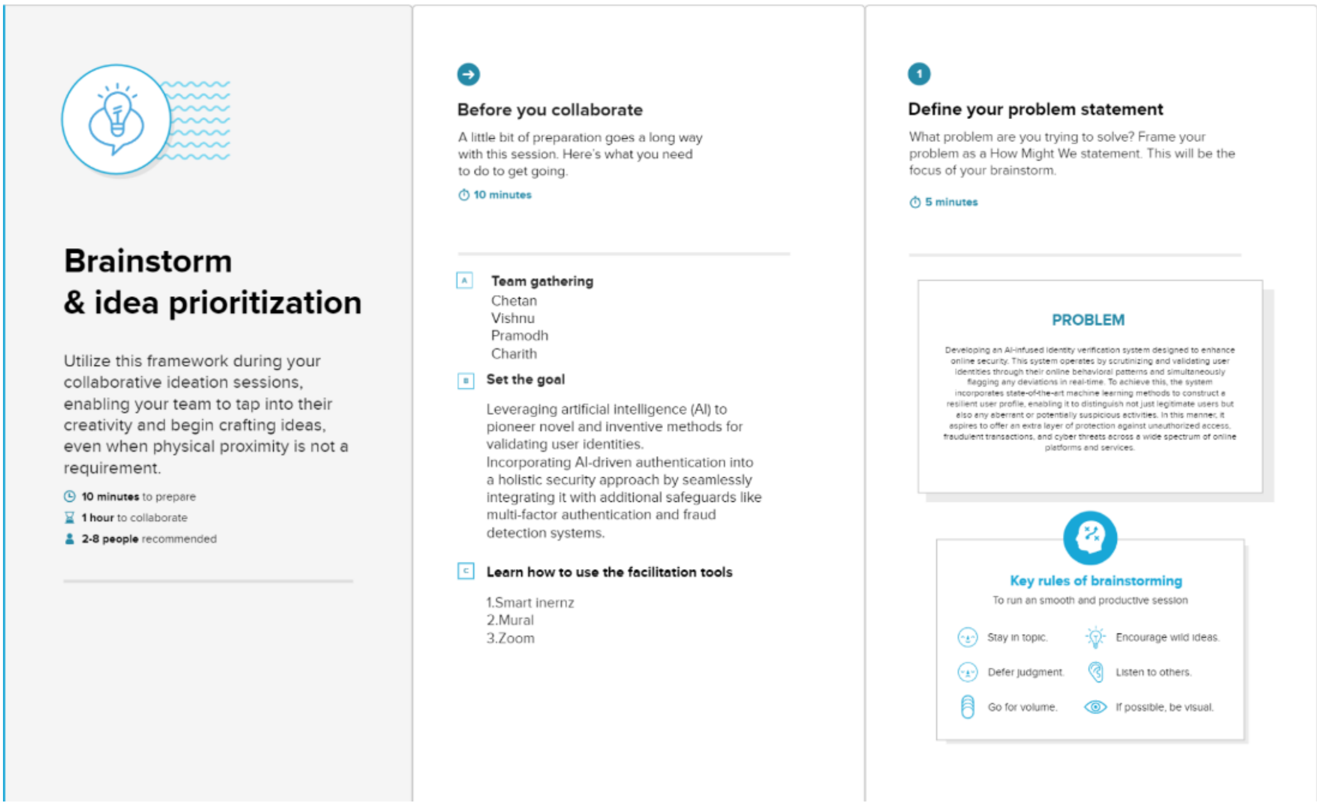
# Ideation Phase
## Brainstorm & Idea Prioritization

| | |
|---|---|
| Date | 19 September 2022 |
| Team ID | 4.2 |
| Project Name | Network Anomaly Detection |
| Maximum Marks | 4 Marks |

**Brainstorm & Idea Prioritization:** 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.

**Reference:**https://app.mural.co/t/networkanomalydetectionproje1811/m/networkanomalydetectionproje1811/1697631569368/1a1547d2df9dac38793cdddb69b6a88d404bd4c1?sender=u4d7d1d67606790fe37743754

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



**Brainstorm & idea prioritization**

Utilize this framework during your collaborative ideation sessions, enabling your team to tap into their creativity and begin crafting ideas, even when physical proximity is not a requirement.

- **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**

Chetan
Vishnu
Pramodh
Charith

B **Set the goal**

Leveraging artificial intelligence (AI) to pioneer novel and inventive methods for validating user identities.
Incorporating AI-driven authentication into a holistic security approach by seamlessly integrating it with additional safeguards like multi-factor authentication and fraud detection systems.

C **Learn how to use the facilitation tools**

1.Smart inernz
2.Mural
3.Zoom

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**

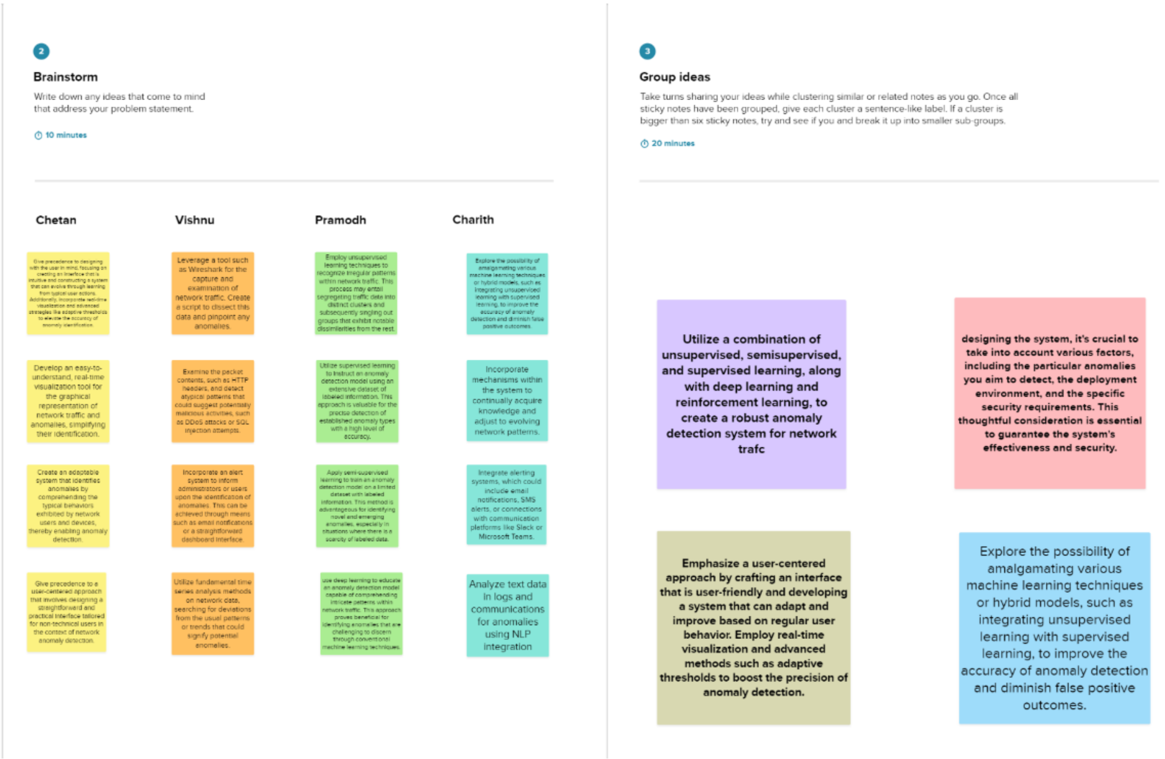
Developing an AI-infused identity verification system designed to enhance online security. This system operates by scrutinizing and validating user identities through their online behavioral patterns and simultaneously flagging any deviations in real-time. To achieve this, the system incorporates state-of-the-art machine learning methods to construct a resilient user profile, enabling it to distinguish not just legitimate users but also any aberrant or potentially suspicious activities. In this manner, it aspires to offer an extra layer of protection against unauthorized access, fraudulent transactions, and cyber threats across a wide spectrum of online platforms and services.

**Key rules of brainstorming**

To run an 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

**Chetan**

Give precedence to designing with the user in mind, focusing on creating an interface that is intuitive and constructing a system that can evolve through learning from typical user actions. Additionally, incorporate real-time visualization and advanced strategies like adaptive thresholds to elevate the accuracy of anomaly identification.

Develop an easy-to-understand, real-time visualization tool for the graphical representation of network traffic and anomalies, simplifying their identification.

Create an adaptable system that identifies anomalies by comprehending the typical behaviors exhibited by network users and devices, thereby enabling anomaly detection.

Give precedence to a user-centered approach that involves designing a straightforward and practical interface tailored for non-technical users in the context of network anomaly detection.

**Vishnu**

Leverage a tool such as Wireshark for the capture and examination of network traffic. Create a script to dissect this data and pinpoint any anomalies.

Examine the packet contents, such as HTTP headers, and detect atypical patterns that could suggest potentially malicious activities, such as DDoS attacks or SQL injection attempts.

Incorporate an alert system to inform administrators or users upon the identification of anomalies. This can be achieved through means such as email notifications or a straightforward dashboard interface.

Utilize fundamental time series analysis methods on network data, searching for deviations from the usual patterns or trends that could signify potential anomalies.

**Pramodh**

Employ unsupervised learning techniques to recognize irregular patterns within network traffic. This process may entail segregating traffic data into distinct clusters and subsequently singling out groups that exhibit notable dissimilarities from the rest.

Utilize supervised learning to instruct an anomaly detection model using an extensive dataset of labeled information. This approach is valuable for the precise detection of established anomaly types with a high level of accuracy.

Apply semi-supervised learning to train an anomaly detection model on a limited dataset with labeled information. This method is advantageous for identifying novel and emerging anomalies, especially in situations where there is a scarcity of labeled data.

use deep learning to educate an anomaly detection model capable of comprehending intricate patterns within network traffic. This approach proves beneficial for identifying anomalies that are challenging to discern through conventional machine learning techniques.

**Charith**

Explore the possibility of amalgamating various machine learning techniques or hybrid models, such as integrating unsupervised learning with supervised learning, to improve the accuracy of anomaly detection and diminish false positive outcomes.

Incorporate mechanisms within the system to continually acquire knowledge and adjust to evolving network patterns.

Integrate alerting systems, which could include email notifications, SMS alerts, or connections with communication platforms like Slack or Microsoft Teams.

Analyze text data in logs and communications for anomalies using NLP integration

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

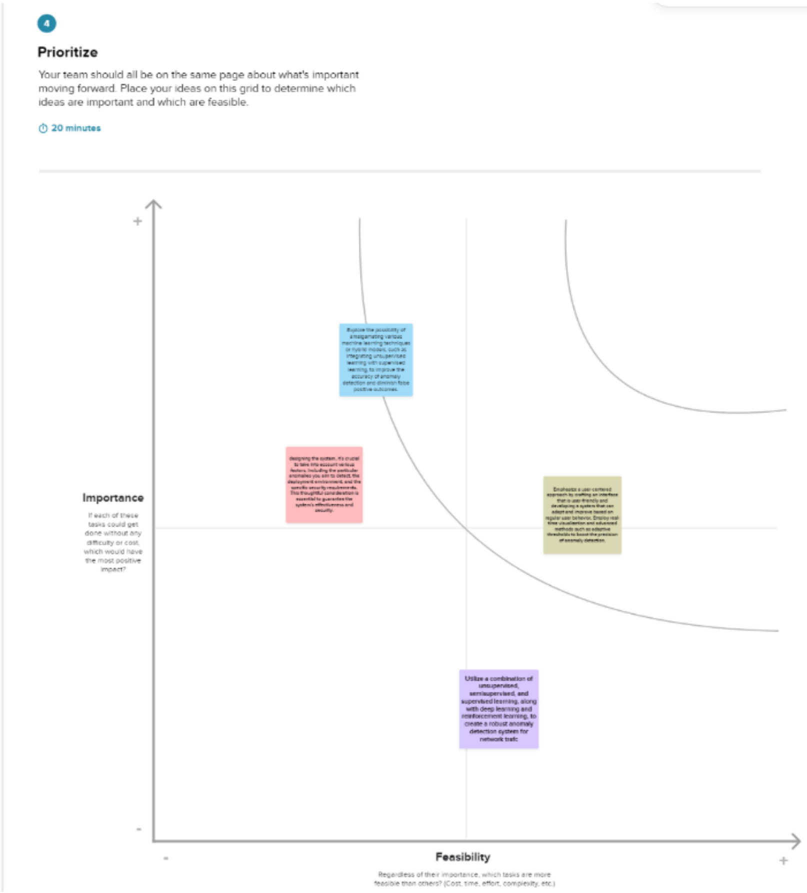
**Utilize a combination of unsupervised, semisupervised, and supervised learning, along with deep learning and reinforcement learning, to create a robust anomaly detection system for network trafc**

**designing the system, it's crucial to take into account various factors, including the particular anomalies you aim to detect, the deployment environment, and the specific security requirements. This thoughtful consideration is essential to guarantee the system's effectiveness and security.**

**Emphasize a user-centered approach by crafting an interface that is user-friendly and developing a system that can adapt and improve based on regular user behavior. Employ real-time visualization and advanced methods such as adaptive thresholds to boost the precision of anomaly detection.**

Explore the possibility of amalgamating various machine learning techniques or hybrid models, such as integrating unsupervised learning with supervised learning, to improve the accuracy of anomaly detection and diminish false positive outcomes.

## Step-3: Idea Prioritization



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

+
Importance
If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?
-
-
Feasibility
Regardless of their importance, which tasks are more feasible than others? (Cost, time, effort, complexity, etc.)
+

Explore the possibility of amalgamating various machine learning techniques or hybrid models, such as integrating unsupervised learning with supervised learning, to improve the accuracy of anomaly detection and diminish false positive outcomes.

designing the system, it's crucial to take into account various factors, including the particular anomalies you aim to detect, the deployment environment, and the specific security requirements. This thoughtful consideration is essential to guarantee the system's effectiveness and security.

Emphasize a user-centered approach by crafting an interface that is user-friendly and developing a system that can adapt and improve based on regular user behavior. Employ real-time visualization and advanced methods such as adaptive thresholds to boost the precision of anomaly detection.

Utilize a combination of unsupervised, semisupervised, and supervised learning, along with deep learning and reinforcement learning, to create a robust anomaly detection system for network trafc