[Krupaben Kothadia](mailto:kkothadi@asu.edu)

* **Data Preprocessing:**
  + Discussing the various preprocessing and NLP techniques to produce a robust dataset for detection of suspicious activities on social media. [10] [11] [12] [13] [14]

[Gautham Vijayaraj](mailto:gvijaya6@asu.edu)

* **Secure Data Collection Techniques:**
  + Finding the right balance between monitoring or detecting suspicious activity or threats in Social media and respecting the user's privacy to maintain ethics, data confidentiality and integrity is crucial while dealing with real data. [5] [6] [7] [8] [9]

[Avani Mundra](mailto:amudra@asu.edu)

* **Data Mining Techniques to Handle Multimodal Data:**
  + The data obtained from Social Media can be unstructured and varied as it can contain texts, images, videos and more. So we need to find a data mining technique that can help us process and analyze suspicious activity. [15] [16] [17]

[Justin Young](mailto:jtyoun15@asu.edu)

* **Ensuring Model Security:**
  + Discussion on techniques producing a secure machine learning detection model which can refrain from tampering or unauthorized modifications from hackers. [32] [33] [34] [35]

[Anuranjan Dubey](mailto:adubey37@asu.edu)

* **Leveraging Machine Learning Models:**
  + Specific machine learning algorithms have been previously employed to enhance the accuracy and efficiency of the proposed tools in the previous research in classifying and categorizing security-related content from Twitter. Research will be performed on whether these algorithms be extended beyond their initial implementation on Twitter, and if they can be adapted for use on other social media platforms with minimal modifications. [18] [19] [20] [21]

[Rahul Nayak](mailto:rrnayak@asu.edu)

* **Data Exploration:**
  + There are a wide variety of suspicious activities that go on social media these days. Thus it is important that we study the different types of suspicious activities. [1] [2] [3] [4]

[Sangeeth Santhosh](mailto:ssantho9@asu.edu)

* **Model Evaluation:**
  + The suspicious social media accounts to be analyzed need to be found correctly without incorrectly grouping non-suspicious accounts as suspicious. Such incorrect classification would mean questioning the integrity of an honest user. Research will be performed on whether the right approach can be found to classify social media accounts into suspicious or non-suspicious without false grouping. [27] [28] [29] [30] [31]

[Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu)

* **Zero-day Detection:**
  + The concept of zero-day detection and its significance in staying ahead of evolving tactics used by malicious actors will be represented by studying various machine learning algorithms based on this concept. [22] [23] [24] [25] [26]