Release 0 , Week 1 |Minutes/Report

## 23/09/2019 | 10:00am | Location: NYP@SIT L4B / NYP@SIT UoG Office

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Meeting called by | Rech Leong | | Type of meeting | Requirements Gathering | | Note taker | Rech Leong | |  |  | | Attendees Rech Leong  Prof. Sye Loong |

# Agenda topics

* + - Requirements Gathering
      * Meeting with Prof. Sye Loong at 2pm
        + To find out more about project scope
        + To understand what is expected of the student(s)
        + To understand the problem domain before undertaking of tasks
        + Questions to ask:

What are the automated systems to be studied/discussed in this project?

What are the relevant research that needs to be done?

Are there any existing research material that applies to the problem domain?

Is there any development needed for this project?

What is expected of the current milestone and the next milestone?

|  |  |  |
| --- | --- | --- |
| Notes and Suggestions |  |  |

* First Milestone (4 to 5 weeks)
  + Research on adversarial attacks on machine learning systems
    - How they were done
    - What hardware/software they used
    - What were the impacts of these attacks
    - Why were these done
  + Progress Report
    - With references and links to the relevant research papers
    - Time spent each day
  + Based on Research findings
    - What is the scope we want to use for demonstration
    - What hardware do we need
* Subsequent Milestones
  + Based on scope identified
    - Determine the possible ways to attack the system
    - Perform these attacks
    - Mitigate these attacks
  + Identify why these attacks happen and how to mitigate them in order to
    - Determine the benefits
      * Identify repercussions possible
      * Justify why it is necessary to mitigate these attacks

|  |  |  |
| --- | --- | --- |
| Decisions |  |  |

|  |  |  |
| --- | --- | --- |
| Action items | Person responsible | Deadline |
| Document Requirements | Rech Leong | 23/09/2019 | 5:00pm |
| Document Project Scope | Rech Leong | 23/09/2019 | 5:00pm |
|  |  |  |
| Research on adversarial attacks thus far and how they were done | Rech Leong | 26/09/2019 | 5:00pm |

**PICTURES OR ANY OTHER RELEVANT RESOURCES**



