AUT

AI for CyberSecurity Project

The 'AI for CyberSecurity Project' originally started in Semester 1 2020 and concluded in the end of Semester 2 2020. It is a research based project that focuses on identifying and describing Use Cases for applying Artificial Intelligence (AI) as a Cyber Security defence mechanism in Medium to Large sized organizations. It also considers and discusses AI methods and approaches that can be implemented in the Use Cases that will be identified, the practical implementation, feasibility and it also includes any issues or challenges related to them.
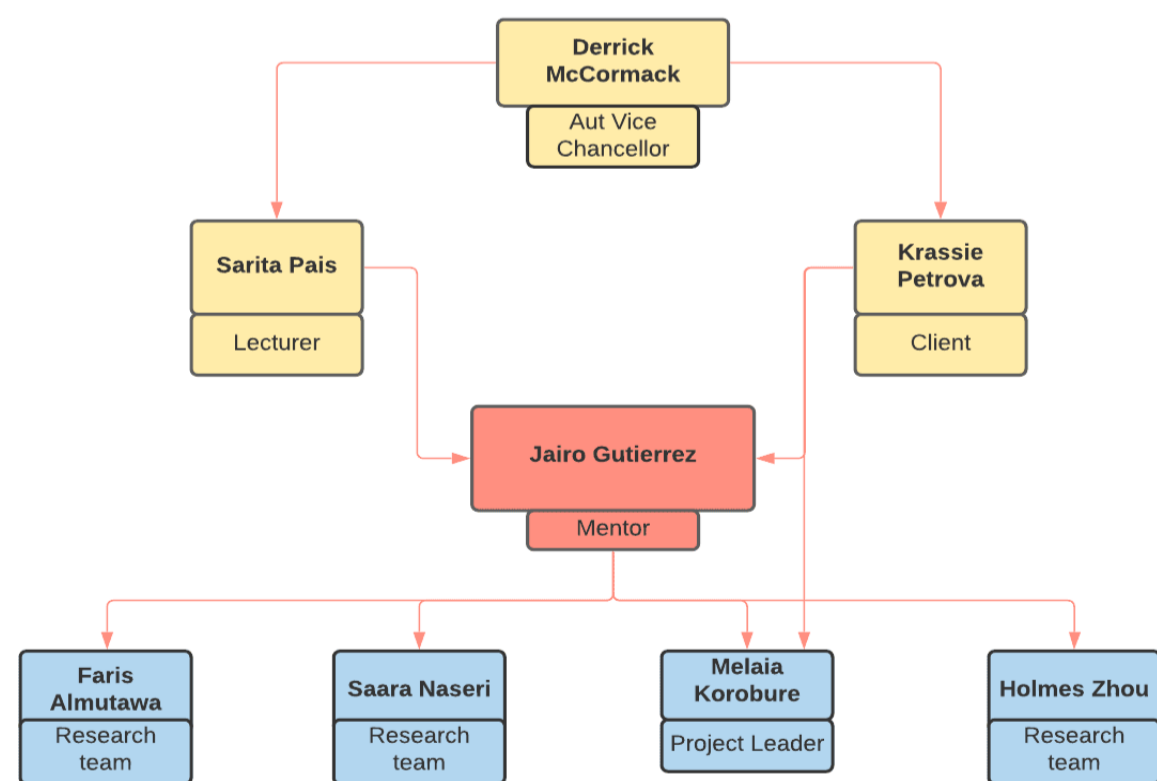
Initiation

Steps taken for Initiation Phase:

1. Project Manager scheduled an Initial client meeting with the Project Team.
2. Another meeting was scheduled to discuss team roles.
3. Our client and mentor shared a few tips on how to execute a successful research and which resources to use and how to use it.

Planning

Steps taken for Planning phase:

1. Decided as a team to utilize Trello and the Gantt chart as Project Management tools.
2. We agreed to schedule Team meetings once every week on Fridays.
3. We agreed to schedule meetings with the mentor ever 2-3 weeks
4. We also agreed to schedule client meeting ever month or once or twice per semester.
5. We discussed which communication platform would be suitable for our team.
6. Tasks were also allocated out equally.
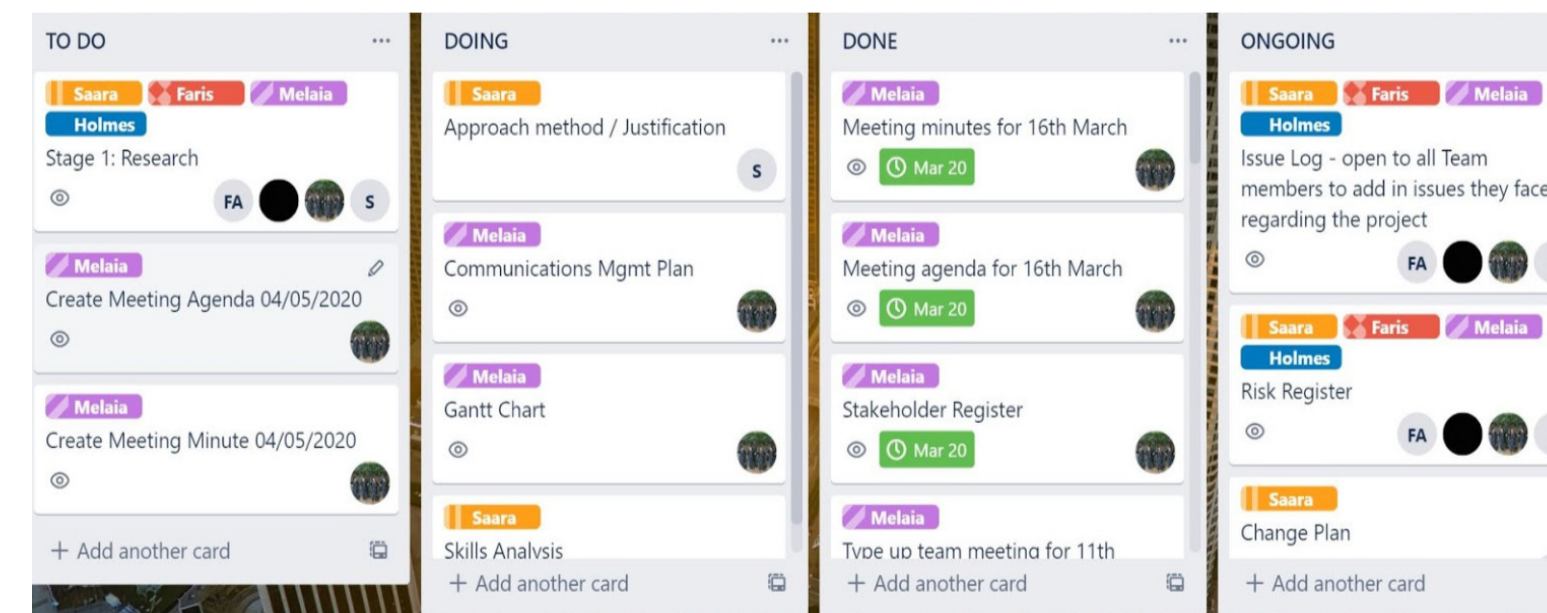
Implementation

Steps taken for Implementation Phase:

1. Team meetings took place every once week.
2. Meeting minutes and agenda will be done before and after every meeting.
3. Ongoing tasks would be updated everytime there's changes.
4. Tasks would be put up on Trello and it would be moved to the 'DONE' section when task is completed.
5. Team Communications would happen through social media and any other communications would happen via email.
6. We used AUT Library and also Google scholar for academic research.

Quality Assurance
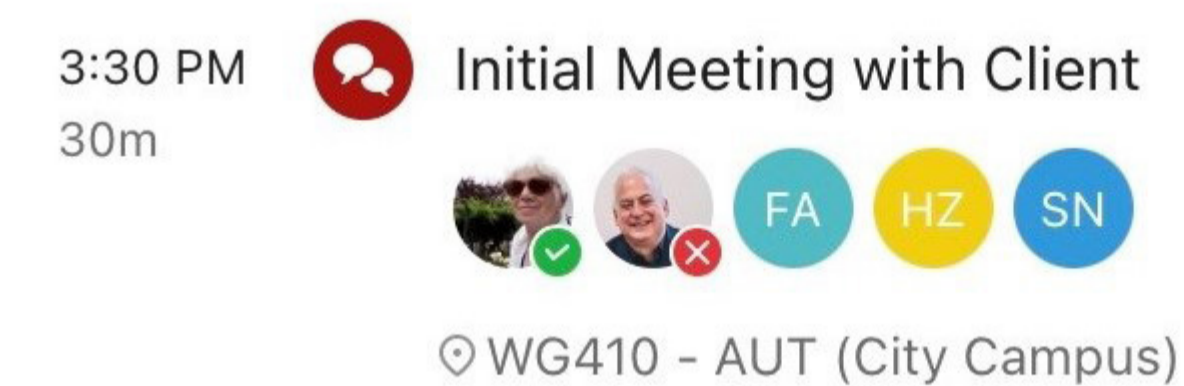
Quality Over Quantity
We ensured that the Case studies chosen for our report was top quality, we decided as a team to aim for find a maximum of 50 Use Cases/Case studies, which enables us to write an in depth report about it.

Feedback
To maintain the quality of our documentation and report we made sure we submitted it to our client and/or mentor 1-2 weeks prior to due date so that we can get some feedback and make changes if needed.

Research and report outline
We published a research and report guildeline to ensure that we as a team are researching valid information for our report.

Project Challenges

1. Lack of Team Communications: We have experienced lack of communication within the project team, whether it is via email, text message or via social media. When this happens it hinders the project team code of ensuring that there is an open line of communication within the project team members.
2. Another challenge is due to COVID 19 hitting New Zealand and causing the whole country to go into complete lockdown this meant that we had to postpone all of our face to face Team meetings with our mentor and our client till further notice. This was also a challenge as we might have become too distracted.

Project Learnings

1. Throughout our project, we were able to learn about AI for Cyber Security and its benefits of use in this modern day, specifically for medium to large sized organisations. Along the way we learnt new research skills and were able to work well in a team to share our knowledge and produce a well researched report to present to our client.
2. Throughout the course of our Case Study research we also learned about the amount of medium to large organizations that are actually utilising Artificial Intelligence within their organisation as a Cyber security defence mechanism.