How to build a trusted AI system for HDB

Internal governance structures and measures

This section of the model AI government framework of Singapore describes how to manage the use of AI in an organisation. This is done by adding specialised departments or adapting existing ones to manage the use of AI in the organisation.

As such, we will be adding a department of AI risk management to the HDB project. This department will be have staffs equipped with the necessary skills and expertise to oversee the implementation of AI models into our project.

This department will have clear responsibilities as required by the framework. These responsibilities are generally to oversee the entire process of AI integration.

As such, the AI risk management department will be incharge of ensuring that the datasets chosen for training purposes are ethical. The dataset should also not have many biases or inaccuracy. It is to the framework’s understanding that no dataset is truly unbias or inaccurate. However, this department should strive to gather the best data for the model’s purpose

Another department that we will be adding is the department of AI research. This department can be apart of the research and development department in our team.

This department will be incharge of ensuring that the staff in all AI departments inside the organisation are fully aware of their role and responsibility within the department. This department is also tasked with providing the necessary resources for the staffs in the AI departments to carry out their job.

Therefore, after referencing the internal governance structures and measures of the framework. This is how I would structure the departments in the organisation responsible for this project.

Level of human involvement in AI decision making

This section of the model AI government framework of Singapore describes how to decide on the level of human involvement in the AI model’s decision making process.

This section is based on many factors like the feature that we will be implementing and the decision of the risk management department. Due to the lack of these factors, we will assume. That we will design a facial detection system to identify residents entering the building’s lift. In my opinion, the risk system would be very high. However, the system should be able to operate efficiently as many people enter the lifts in HDBs.

There are three approaches identified by the government.

The first being Human-In-The-Loop. In summary, this approach suggests that a human must verify every action that the AI is about to do before it does it. An example would be to give a diagnosis for a patient. A doctor should be on stand by to check the diagnosis before it is given out.

The next one being Human-out-of-the-loop. In summary, this approach suggests that there is no human involvement at all. An example, would be product recommendation systems

Lastly, is Human-over-loop. In summary, this approach suggests that a human should be able to take control of the AI when an anomaly occurs.

As such, I would suggest that we use a human-over-loop. This gives a balance between security and speed.

Therefore, this concludes how I would build an system that is trustable for HDB