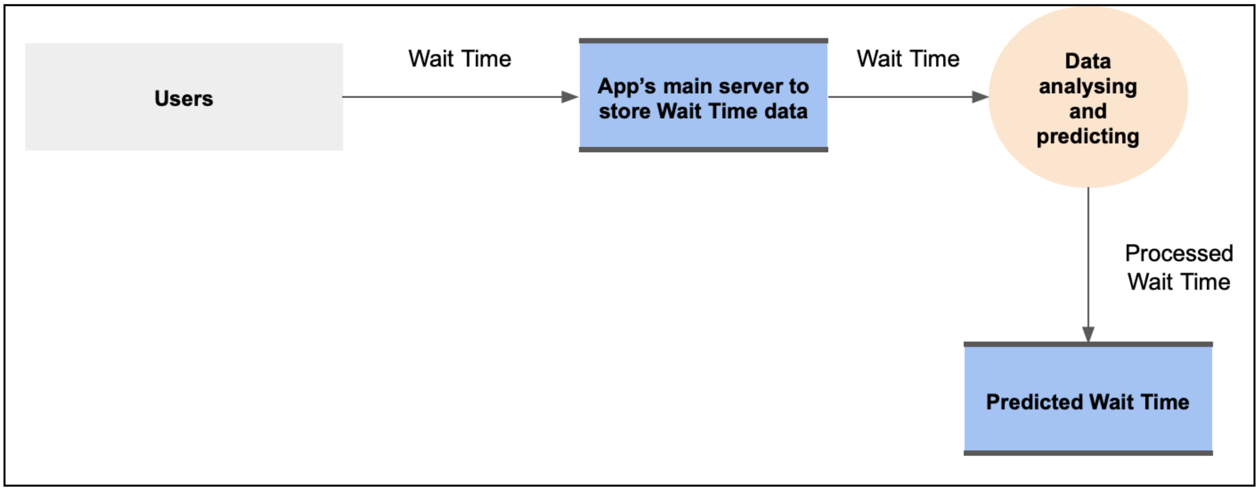
NUS
National University
of Singapore

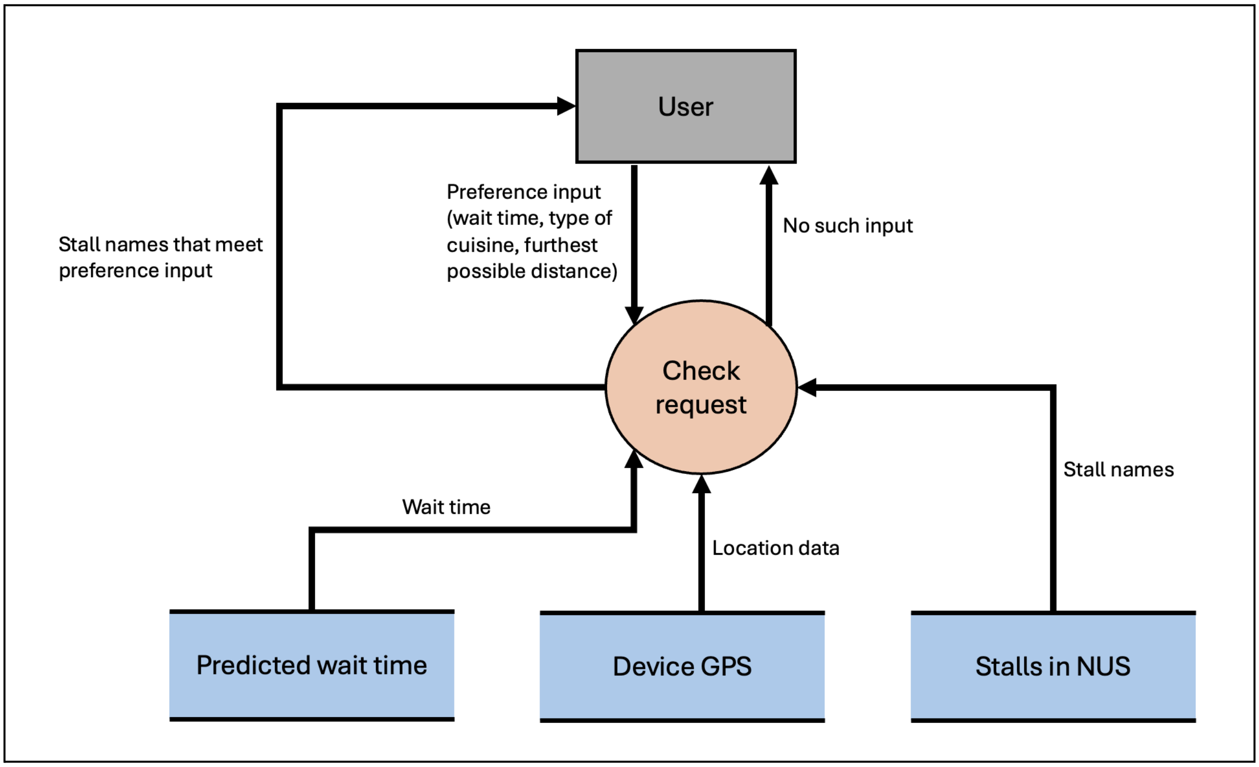
NPS2001C Group Milestone 2

Ideation and Planning Report

Name	**Matric Number**
Hiong Ding Xian	A0252474A
Cassandra Ong Soong Yee	A0253150U
Phoebe Heng Zhiyi	A0258674M
Hu Xinhe Joanne	A0256994H

1. What data does your app need to function and how will your app process it?
    a. Data flow diagram


Users
Wait Time
App's main server to store Wait Time data
Wait Time
Data analysing and predicting
Processed Wait Time
Predicted Wait Time


User
Stall names that meet preference input
Preference input (wait time, type of cuisine, furthest possible distance)
No such input
Check request
Stall names
Wait time
Location data
Predicted wait time
Device GPS
Stalls in NUS

Users will input their wait time at the stalls they are at. This wait time will be processed and end up in a database 'Predicted wait time'. The 'Predicted wait time', 'Device GPS' and 'Stalls in NUS' will be used to filter out the stall names that meet the user's preference input.

2. What are the issues related to data privacy and security for your app and how will your app deal with them?

As mentioned in the previous section, the app will mainly collect the following personal data:

1) Food preferences

Data is collected manually, meaning users have to input their food preferences into the app themselves and can change the settings anytime. This data is used for food recommendation.

2) Real-time location

Data is collected automatically, unless users opt out by updating their location tracking permissions. This data is used for filtering recommendations based on distance from user's location. This function will be limited should users opt out.

3) Past activities on the app – eg. History of food places searched

Data is collected both automatically and manually. Users can save their most frequented food places to favourites, or algorithms will track their app history to understand the user's preferences.

Some of the security and privacy risks associated with the app are:

Risks	Elaboration	Mitigations
Insecure Authentication	App does not require users to set up a (complex) password, making it easy for hackers to access sensitive data. This introduces the risk of **loss of confidentiality.**	Do not collect sensitive user data. Only minimal data collection such as understanding users' food preferences. Should any sensitive data be collected, enforce a minimum of 12 characters for the password.
Invasion of privacy with location tracking	Location tracking records users' real time location. Thus, individuals may unnknowingly expose sensitive information about their whereabouts, routines and personal preferences. This introduces a risk of **loss of confidentiality.**	Be transparent and allow users to update their tracking permissions anytime Eg. Only track when using the app. Allow clearing of location data.
Biased or inaccurate crowdsourced data	Crowdsourcing collects data from a large pool of anonymous contributors. This introduces a risk of **loss of integrity** when contributors feed the system biased or inaccurate data (Eg. exaggerating the wait	Having a system in place for verification of data. For example, periodic ratings such as "how accurate/ reliable was the wait time"

	time because they are impatient with waiting).	can be asked of users. This allows cross checking of data.
Malware distribution	Attackers may attempt to distribute malware through malicious links or files shared through the app. This introduces a risk of **loss of integrity.**	Implement strict code review processes to identify and eliminate potential vulnerabilities and malicious codes. Promptly release security updates to address newly discovered vulnerabilities and mitigate emerging threats.

We analyze the extent of the risks using the risk assessment matrix below:

Likelihood	Impact			
		Mild	**Moderate**	**Severe**
	Near Certain	Medium	High	High
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium

SYSTEM:			
Threat Event	Likelihood	Impact	Risk Level
Loss of Confidentiality	Likely	Moderate	Medium
Loss of Integrity	Likely	Moderate	Medium
Loss of Availability	Unlikely	Low	Low
		OVERALL RISK:	Medium

Link to github repository:
https://github.com/thedingdude/NPS-Group-Project