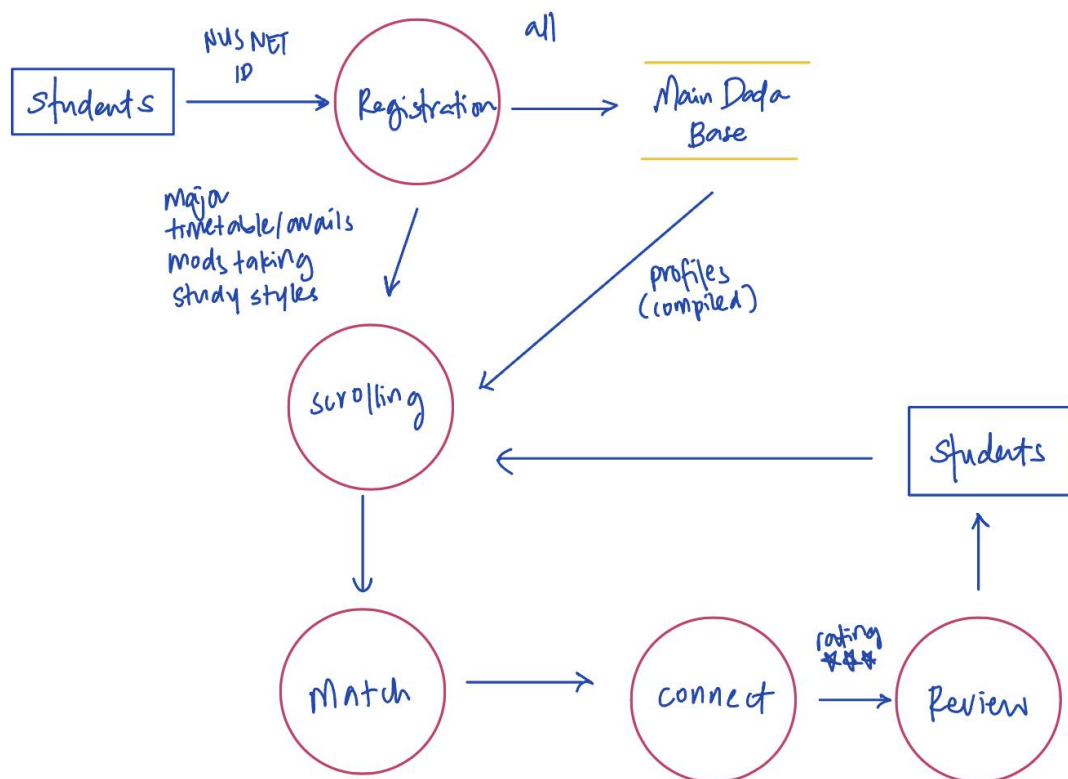


Vritee Muni (A0264771X)
Tasneem Binte Jamaludeen (A0255684R)
Evangeline (A0255488M)
Julie Lo Smithgul (A0264787J)

1. For registration, the user's name, NUSNET ID and NUS email are needed.
For preliminary matchmaking, the user's major, year of study, gender and age are needed.
For further matchmaking, the user's modules, study styles, availability and preference for in-person or online meetings are needed.



2. Given our app's interactive platform and user interface, there may arise significant privacy and security concerns, and thus it may be necessary to safeguard the app from data breaches and theft. As the app collects personal data (ie. name, age, email address, major, etc.) to aid the matching process of study buddies, it may lead to privacy issues as such information is considered sensitive. Collection of sensitive information also leads to security issues as our app would be more vulnerable to data breaches as it becomes a target for hackers, who want to gain access to personal/confidential information of users. Our app will be designed to deal with these issues by encrypting the data collected, especially personal data, in order to prevent unauthorised access.

In the context of our app, the collection of user data will only be performed upon gaining their consent. Users will be required to provide explicit consent for data collection and usage when they create their profiles. They will also be informed of how their data will be used to facilitate study group formation and


will not be shared with any third parties without explicit user consent, except in cases where it's necessary for study group formation. Lastly, in terms of sharing personal data, users will have control over the visibility of their profiles. They can choose to make certain information public while keeping other details private. Additionally, users will be able to report issues related to harassment and misuse as well as have the option to delete their accounts and associated data at any time.

For protection of data in the data collection process, at first, the app must include strong encryption protocols as well as multi-factor authentication systems to verify user identities. Furthermore, given the straightforward system of the app, minimal data will be collected, avoiding any sensitive or irrelevant data being collected or used. Privacy settings must also be included at the granular level, in the architecture of the app, to allow users to control who can view their profile and who they can share their data with.

For instance, when the user opens the app, they would need to login with their NUSNET ID and password in order to avoid entry by malicious actors, and thus allow for user verification. Additionally, users may be allowed to report another user if they suspect suspicious activity and malicious actors. Lastly, the app will implement strict controls on file upload with validation of file types and checking for malware. Access of files will be limited to authorized users.

Threat Event	Likelihood	Severity	Risk Level
Unauthorised Access	Likely	Severe	High
Data Breach	Unlikely	Severe	Moderate
Inadequate Encryption	Unlikely	Moderate	Moderate
Misuse of Shared Data	Likely	Moderate	Moderate
		Overall Risk:	Moderate

Thus, in order to mitigate these security risks, the app must include well-rounded security assessments, user testing and feedback on security-related issues. In case of a data breach, the app must also be able to identify and notify users of the data breach immediately. Lastly, the app will employ secure practices such as restricting access and using firewalls and intrusion detection systems to protect user activity and data.

Dataset:  NPS2001C_Milestone 2