Question 1

1.1

My target audience are high school staff and students. Firstly, I make user research on each target audience; this allows me to understand the prospective users of my website and to investigate what type of content and features users wanted. By the initial research, I learn that high school staff are teachers and or other school staffs who teach lessons and give feedbacks of student's performance. The students are people who receives feedbacks from their teachers who are high school staff, they are looking for feedbacks to improve their marks. Secondly, I make personas for each target users based on the user research, following the PACT guideline. The persona is an artefact used to make reliable and realistic representations of the target audiences. By using persona, it gives a clear picture of the user's expectorations to developers and it describe real people with backgrounds, goal and values which benefits developers to determine appropriate approaches based on user behaviours. By the results of personas, I know that high school staff are educated with at least university degree, they could be male or female, they are likely to send feedbacks to either other school staffs or to their students, a high school staff may send feedbacks to a lot of people, they want a efficient and effective way to manage such sending. In addition, student's female or males, they are possibly international students or domestic students, they receive feedbacks from different staffs, and they want to have an effective way to store and read such feedbacks.

1.2

The task performed by high school staff includes:

- Account registration when they firstly used the website
- Daily login and logout from the website
- Create a group for other school staffs so they could communicate or give feedbacks with other group members
- They invite students or other staffs to the group
- They send feedback either anonymously or not anonymously to the group
- They can view feedbacks sent by other group members
- Evaluate group cohesion based on feedbacks

The task performed by students includes:

- Account registration when they firstly used the website
- Daily login and logout from the website
- Join groups by invitations sent by high school staffs
- Give feedbacks to other group members
- View feedbacks from other group members
- Evaluate group cohesion based on feedbacks
- Save or download the feedback so they can view it later

1.3

I use the PACT analysis to analyse the context where the website is used by both students and high school staffs. The PACT analysis helps me to think about how target audience interact with the website within certain context and how holistic systems could better visualise actual people and human-computer interaction. In addition, I could use user surveys among target audiences, I could design two surveys which the first one target on high school staff and the second one target on

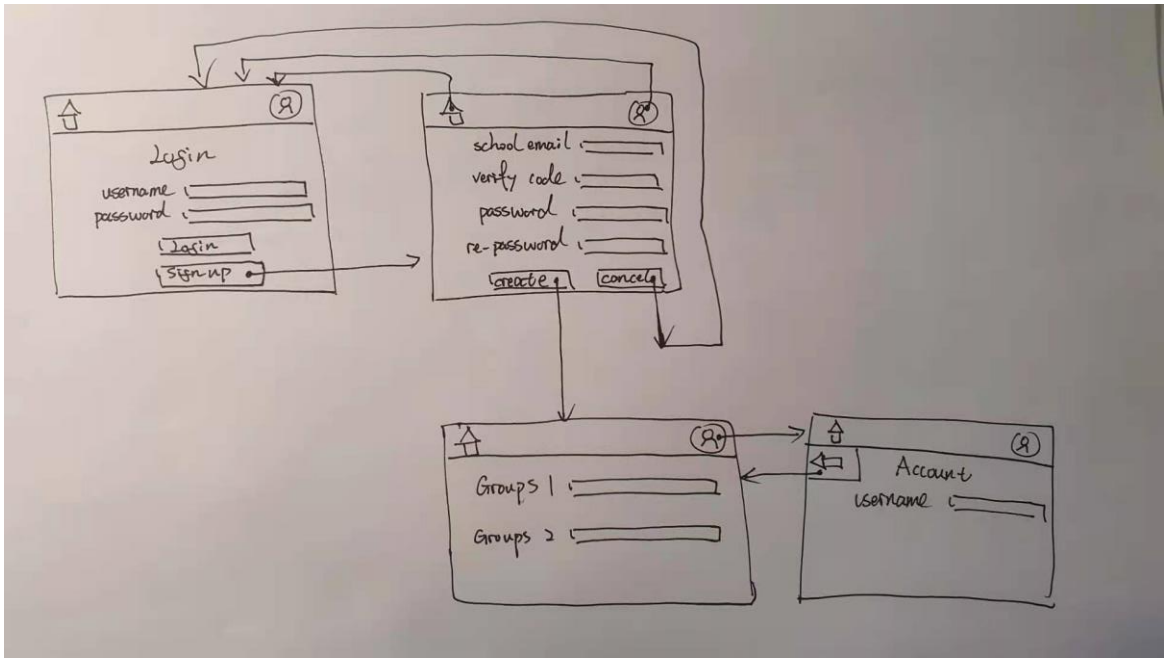
students, the question is about where they use the website and when to use the website. By analysing the results of surveys, we could get a summary of the perspective of target audience and whether people who reluctant to give feedbacks or risk damaging work relationships are caused by the social context.

For people who reluctant to give feedbacks, the reason might be that the system could not provide assurance to protect their identities and make feedbacks fully anonymously. So that, the interface feature should protect their identities whether sending feedbacks or receiving feedbacks. For the suggest interface feature, the user who send the feedbacks could choose the group members to have the rights to view the feedbacks, user that are not assigned have no privileges to view feedbacks, this protects the identities. In addition, the feedback is sent by a system notification instead of by the user themselves, this avoid the identity of the feedback sender being spotted by other members.

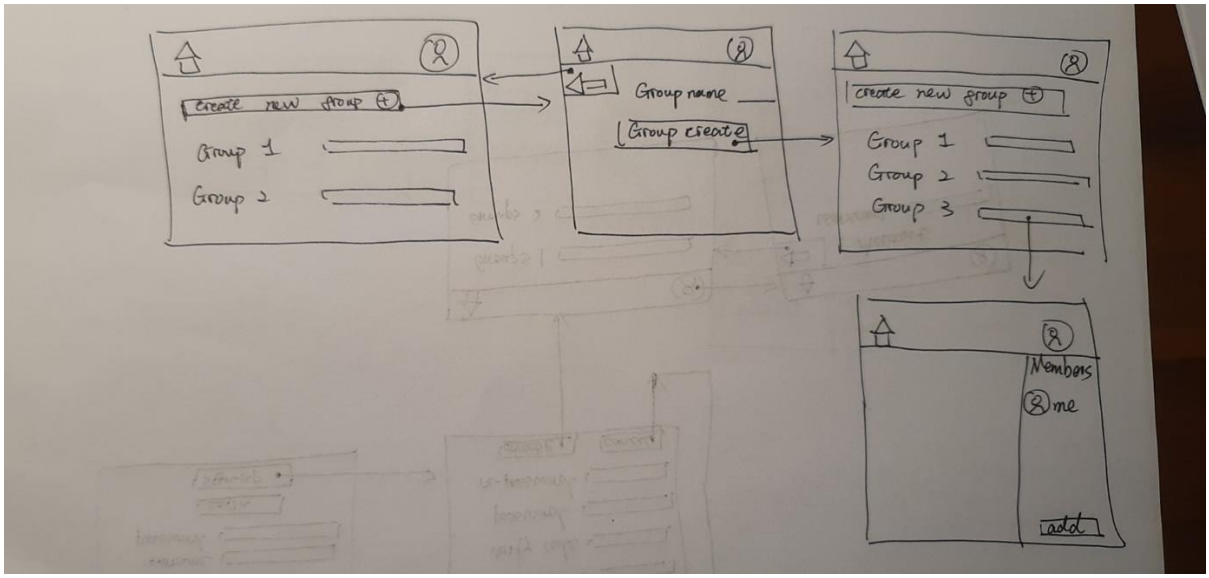
Question 2

2.1

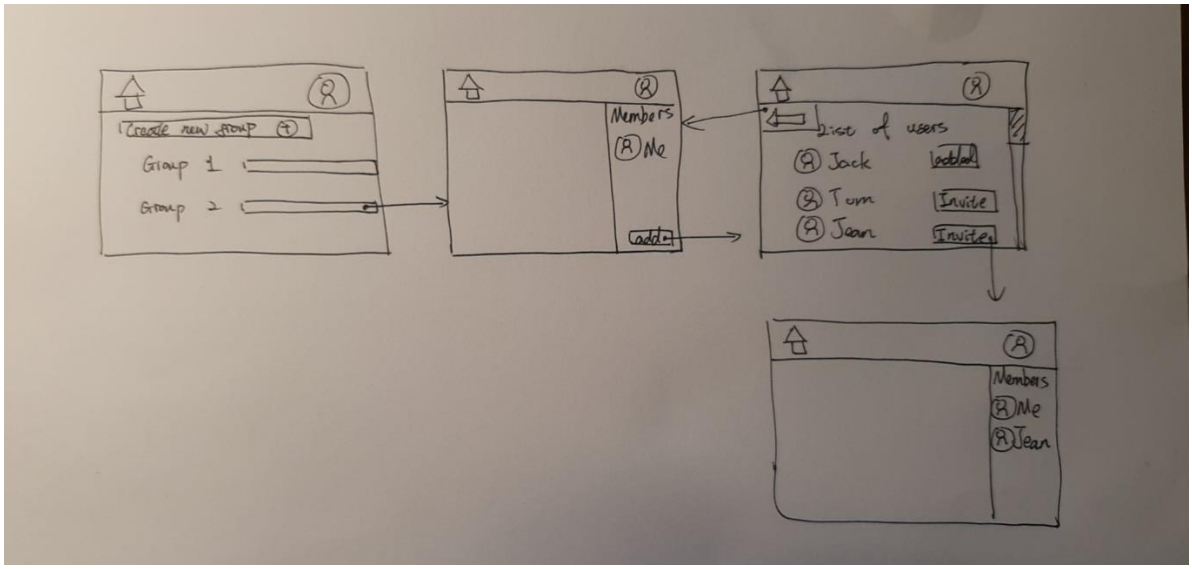
1. For students or high school staff who want to register a new account and login, the wire flow is shown below:



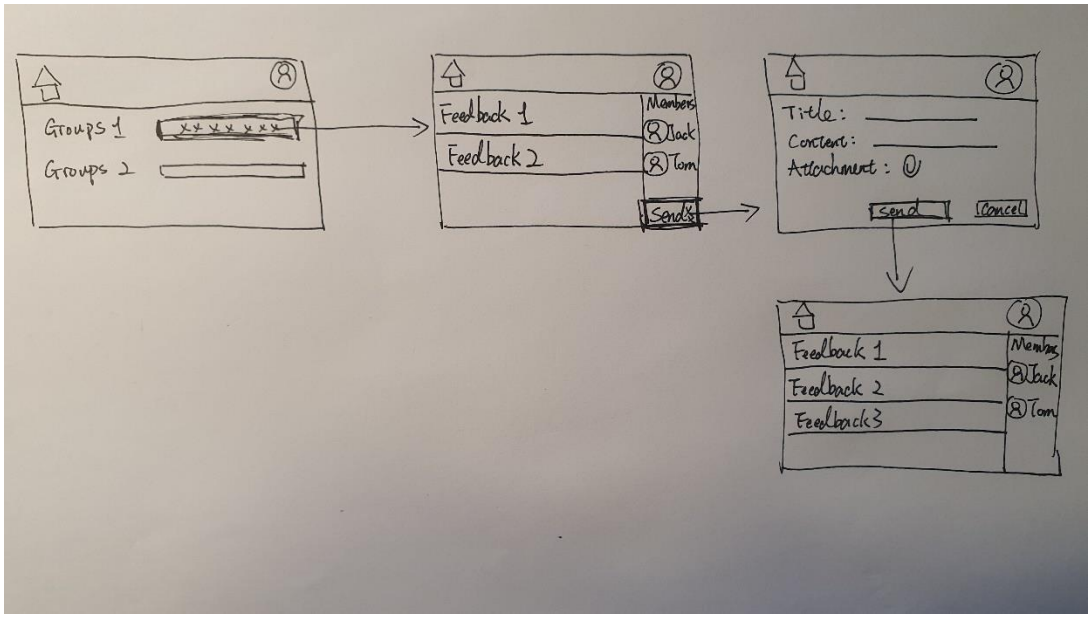
For users who want to create a group:



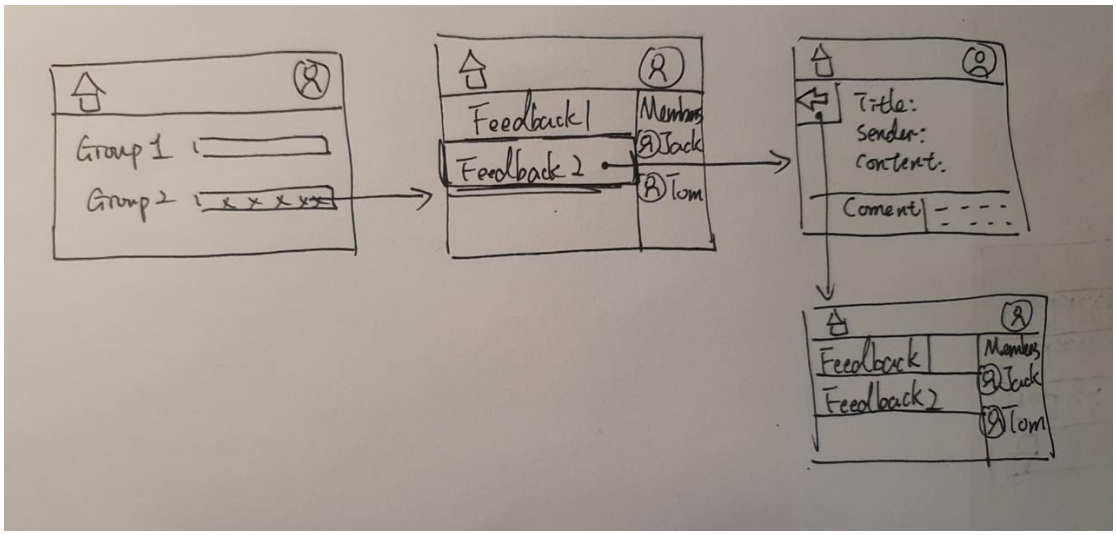
For users who want to invite people into the group:



For students who want to share feedbacks in a group, the wireflow is shown below:



For students who want to view a feedback, the wireflow is shown below:



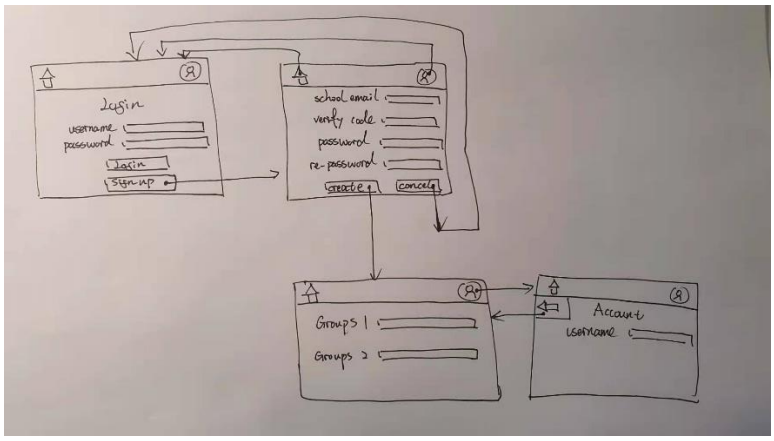
2.2

The interface feature follows the Web Content Accessibility Guideline (WCAG). Firstly, we wisely choose the foreground colour and the background colour to make it distinguishable and easier for users to see, this feature allows users who are colour-blind, sensitive to high contrast colour ratio able to use our website, therefore improving the accessibility. Secondly, we make the website keyboard accessible, this means all functionality on the website are available from a keyboard, this feature makes the input not only dependent on mouse input, therefore improving the accessibility. Thirdly, we make the text content readable by using different font size for the title, the content and footage, as well as choosing the commonly used font that is accepted by majority of people. This make users better understand the text content and make it easier to identify definitions of words.

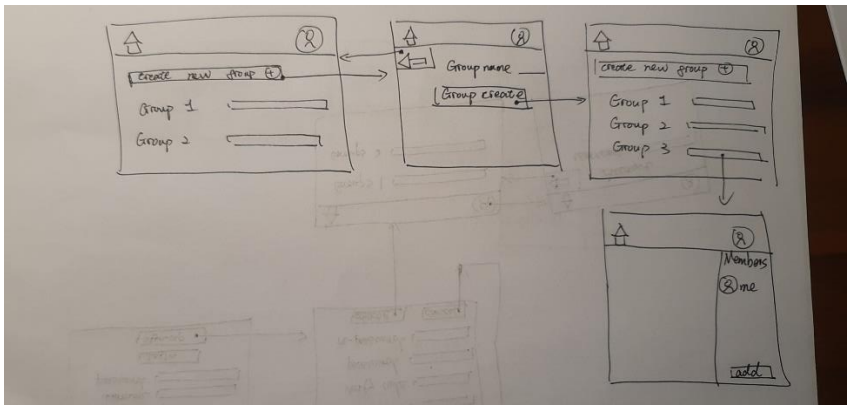
2.3

For the cognitive walkthrough, we are going to ask three questions: Is the sentences succinct, will user recognize action as the correct one, Is the title and headings clear and distinct

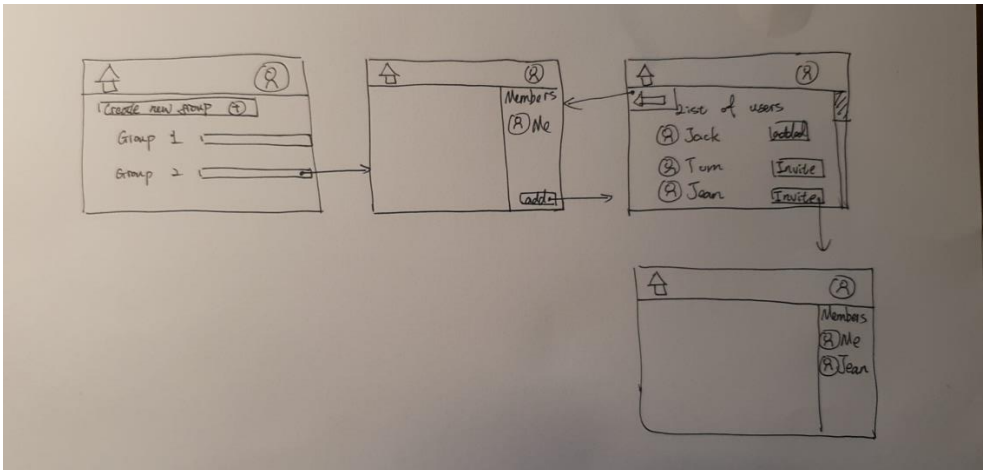
For the registration task, the wireflow is shown below and the result of the cognitive walkthrough is yes, yes, no. During the execution and evaluation, the title text and the content text are not distinguishable, this could let the user confused. To improve this, we should adjust the font size by increase the font size of the Title and position it in an obvious place.



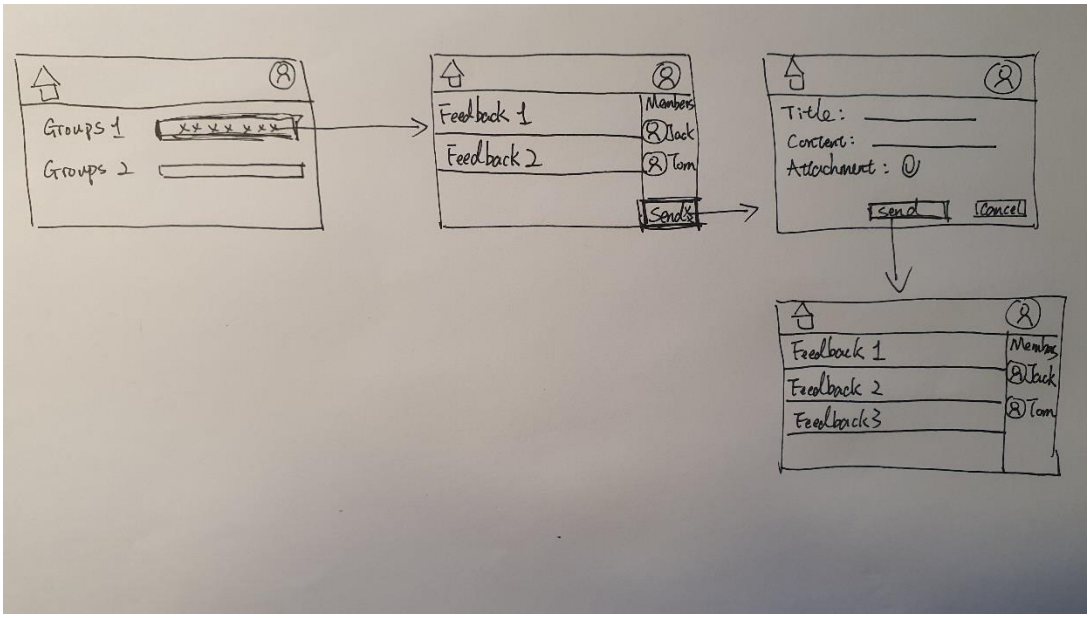
For the Group creation task, the wireflow is shown below and the result of the cognitive walkthrough is no, yes, yes. The sentence “create new group” could be replaced by “create group” with a “+” symbol attached to make it more succinct, the sentence “group create” button is confusing and should change to “next” or “confirm”.



For the task of inviting other users, the wireflow is shown below and the result of the cognitive walkthrough is yes, yes, yes. Therefore, it is sufficient to support users.



For the task of sharing of anonymous group feedback with other members of the group, the wireflow is shown below and the result of the cognitive walkthrough is yes, yes, yes. Therefore, it is sufficient to support users.



Question 3

It is possible to maintain usability while catering a wide user base. As the number of user increases, the number of type of users increased as user various in physical ability, preferences and acceptability. To handle and manage the usability among such wide user base. It is important to categories the common preference and characteristics of users; this allows the developer to develop and make features suitable for majority of users. Besides, guiding users by providing help links in the most obvious place where the user could easily recognize and use it allows more people to understand how the website is structured and how functions works, therefore maintain the usability even with a wide user base. In addition, give the user more options to modify and choose the visualization on the website or the content on the website allows users to customise their experience on the website to maximise the accessibility, the idea behind is to let users determine and choose the most comfort and accessible way while using the website. Therefore, through the above methods we could possibly maintain usability while catering a wide user base

Question 4

4.1.2

The scheme involves two parts. Firstly, the user registered in the site using username and password, this is the first factor authentication. After the registration, the site gives the user a one-time token and requires the user to save the token as a physical evidence, such as write on a paper, this is the second factor. Users are required to use a second factor authentication alongside with username and password when attempting to logged into the site, they will enter their username, password and the token value.

The advantage of using username and password highly depend on the complexity of password pattern and the disadvantage is that for common password, hackers could easily hack by

using rainbow dictionary attack or brute force attack. The advantage of using physical key is that it does not leave digital track on the internet so the hacker could hardly trace and find out the key unless they steal the physical key, this improves the security and relies on how the user protect and secure the physical key in reality. The disadvantage of physical key is that if the key is stolen, then the hacker will forever know the key and make it easier to hack.

4.2

The goal of confidentiality is relevant as we want to limit the accessibility of information to ourselves and keep it protected from others, in other word the information is private and secured. The goal of integrity is relevant as for the physical key, we want to keep it working instead of being replaced by attackers, the integrity directly related to the security of the information. The goal availability is irrelevant as it is the goal of the site providers who manage to provide services. The goal of non-repudiation is irrelevant as we don't need to proof the integrity and the origin of data when we are accessing the site. The goal of auditability and anonymity are irrelevant. The challenges that might occur includes physical key being stolen or copied by attackers, the common password pattern, the leaks of username, password and key in the server database.

4.3

Question 5

5.1

Threat type	Severity Level	Probability of occurrence	Damage level
Rainbow dictionary attack	Medium	High	Medium

Brute force attack is a type of network attack that involves the use of a rainbow hash table, this table contains the values used to encrypt the passwords before and it compares the hash value in the database with the rainbow table hash values when the user attempt to log in. For example, there has been a large number of attempts to login as the admin, the attackers tried different hash values when logging in with the admin username. The attempts are recorded in the log.

Threat type	Severity Level	Probability of occurrence	Damage level
SQL injection	High	High	High

SQL injection attack is a type of network attack that attackers interfere with the queries, such as input bar, to execute SQL statements without authority to the database. The results are server as the attacker obtain the information stored in the database and the database stores all private and important information. An example is that attackers put the query "" OR 1=1; DROP TABLE Users in the input bar and the server will always execute this query as "" OR 1=1 makes the SQL query always true, therefore the table in the database is deleted and information is lost. This could cause serve damage to the server.

Threat type	Severity Level	Probability of occurrence	Damage level

Dos attack	High	High	High

A denial of service attack (DoS) is a type of network attack in which the attacker trying to deny access to the system's network resources to its intended user by disrupting the services of the connection of the host to the internet. For example: An online shopping website is confronting against dos attack which the server computer is being attack and cannot connect to the internet, the attack continuous for 7 days and the website went down during the 7 days, it causes huge final loss.

5.2

For the rainbow dictionary attack, a possible control is to use double salt at the beginning and the end of the string and use complex salt values on username encryption and password encryption and store the encrypted value in the database. This is easy to perform as the time cost for hashing is low. This will increase the difficulty for the attackers to match and get the correct hash value as they are using previously used hash value.

For the SQL injection attack, as the sql injection would cause damage during the execution of the query, then we could prevent such attack by prepared statement so that the query and the data are presented to the database separately. This is sightly complex than the control for rainbow dictionary attack as it modifies the code part of the database and the system controller.

For the DOS attack, a possible control is to identify the ip of the attackers when they perform dos attack and block users from such ip. In addition, as the DOS attack want to utilise all bandwidth, we could increase the bandwidth of the server. Moreover, distributed system could protect the data and the server from the dos attack as it separates the data into different server, it optimises the system and prevents the use of network resources. The effectiveness of distributed system depends on the scale of distribution, the larger the scale of distribution, the more effective the defence.

The ranking of the control of threats is: DOS attack control, SQL injection control and rainbow dictionary attack control, presented in descending order. The higher the ranking place, the higher the priority the development team need to implement the control.

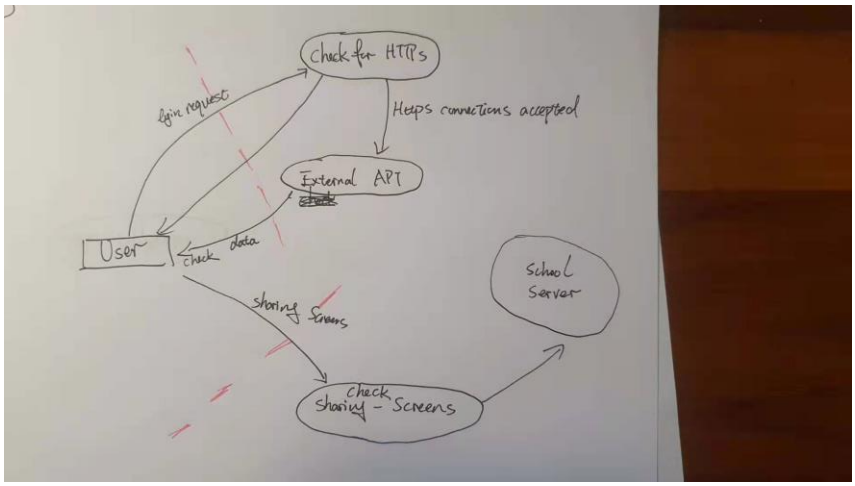
Question 6

6.1

6.2

Potential cheating includes accessing to external materials other than the permitted material from the internet, sharing passwords between students and ghost writers.

The threat model is shown below:



We could use proctorU to monitor the screen the user is using and let the student turn on the camera so that we could check whether the student is browsing or using not permitted external materials. This method could be highly possible to prevent cheating as we monitor the whole answering process. However, the proctorU collects cookies and personal information from the student computer. It might monitor and collect private information that is the student not giving permission and cause offend their privacy, in addition, if the server or database of proctorU has been successfully attacked, it will also cause personal information leak.

Another method is to detect the use of external API o the browsers, if the student opens up facebook on the browsers, we could detect such activities and inform the student that chat is consider as cheating. If the student ignores the warning and carry on using facebook, we then determine the student is cheating. The advantage of the method is that it could rapidly detect the use of external APIs but the disadvantages is obvious it might wrongly detect the API as it relies manual pre-selections of prohibited APIs. Besides, the auto detection of the external API could also read personal information from the browser and the computer, therefore offend students' privacy