COMP225

Group I – Choi, Yeyul; Choi, Jihol; Lee, Jungyu; Seol, Min Young.

Assignment #1 (Part A)

Deliverable #1

Section 1 “Introduction” and sub sections:

1.1 Purpose:

- This new software product will solve the problem of securing users' personal information by preventing Shoulder Surfing. This is version 1.0.0.

1.2 Document Conventions:

Acronyms	Description
SQL	Sequential query language
DB	Database
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheets

1.3 Intended Audience and Reading Suggestions:

- This document is intended for developers, project managers, marketing staff, end users, investors, testers, owner, and documentation writers.

- Section 1: This section is for developers, project managers, investors, owner, and marketing staff.

- Section 2: This section is for developers, investors, owner, and project managers.

- Section 3: This section is for developers, investors, owner, and project managers.

1.4 Project Scope:

Many people are at risk of hacking when they access or store personal information in public places. It is a software that prevents them from the danger of hacking. By using this program, users can safely log in to any service in a public place. The software has the advantage of offsetting the concept of 'key' because it creates a combination of preset colors and numbers of colors. It can have color distortion software to create confusion for people who try shoulder surfing when viewed from a different direction. Keyboard shortcuts help reduce password entry time and increase security as traditional methods do. In particular, the secondary authentication number that comes through text messages when handling money-related tasks is also at risk of hacking, so that part can be prevented.

1.5 References:

Graphical password to avoid shoulder surfing. (2018, November 24). Nevon Projects. https://nevonprojects.com/graphical-password-to-avoid-shoulder-surfing/

더 나은 코드 보안을 위한 5 가지 개발 툴. (n.d.). ITWorld Korea. https://www.itworld.co.kr/news/98638

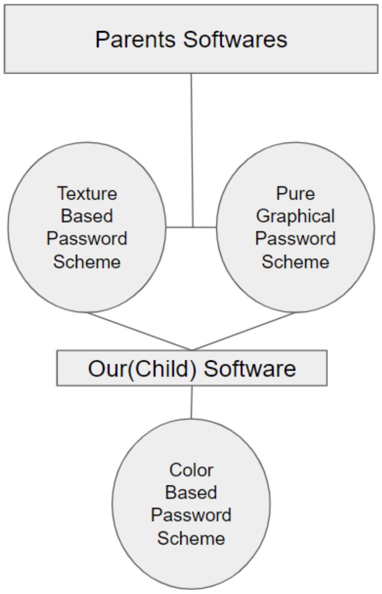
기업에 필요한 18 가지 보안 제어,. (n.d.). ITWorld Korea. https://www.itworld.co.kr/news/195944

소프트웨어 보안: 안전한 모바일 응용 프로그램 만들기. (n.d.). KO.EYEWATED.COM. https://ko.eyewated.com/%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4-%EB%B3%B4%EC%95%88-%EC%95%88%EC%A0%84%ED%95%9C-

%EB%AA%A8%EB%B0%94%EC%9D%BC-%EC%9D%91%EC%9A%A9-%ED%94%84%EB%A1%9C%EA%B7%B8%EB%9E%A8/

Section 2 “Overall description” and sub sections:

2.1 Product Perspective:


Parents Softwares
Texture Based Password Scheme
Pure Graphical Password Scheme
Our(Child) Software
Color Based Password Scheme

2.2 Product Features (Functions):

1. New way to input password: combination of colors, letters and numbers

2. No risk even if you enter the password directly

3. Easy to enter the password according to the location by using the shortcut keys

2.3 User classes and Characteristics:

- People in public places: Will use the new software to access their personal account or working safety in public places

2.4 Operating Environment:

The software:

- will run on a Unix server

- will be developed using C#, HTML, CSS, etc...

- supports the following browsers such as Chrome, Firefox, Microsoft Edge, and Safari

- supports iOS, Android for the mobile version

2.7 Assumptions and Dependencies:

- The software will use colors that have similar hue, saturation, and lightness to enhance security and to apply color distortion software when the screen is viewed from other directions.

- In addition to colors, the software will also use a combination of lowercase letters (from a to h) and numbers (from 1 to 8).

- Three layers of colors, letters, and numbers will consist of one block and be given coordinates according to each position.

- Each coordinate (position) will have keyboard shortcuts to reduce the time it takes to enter the password.

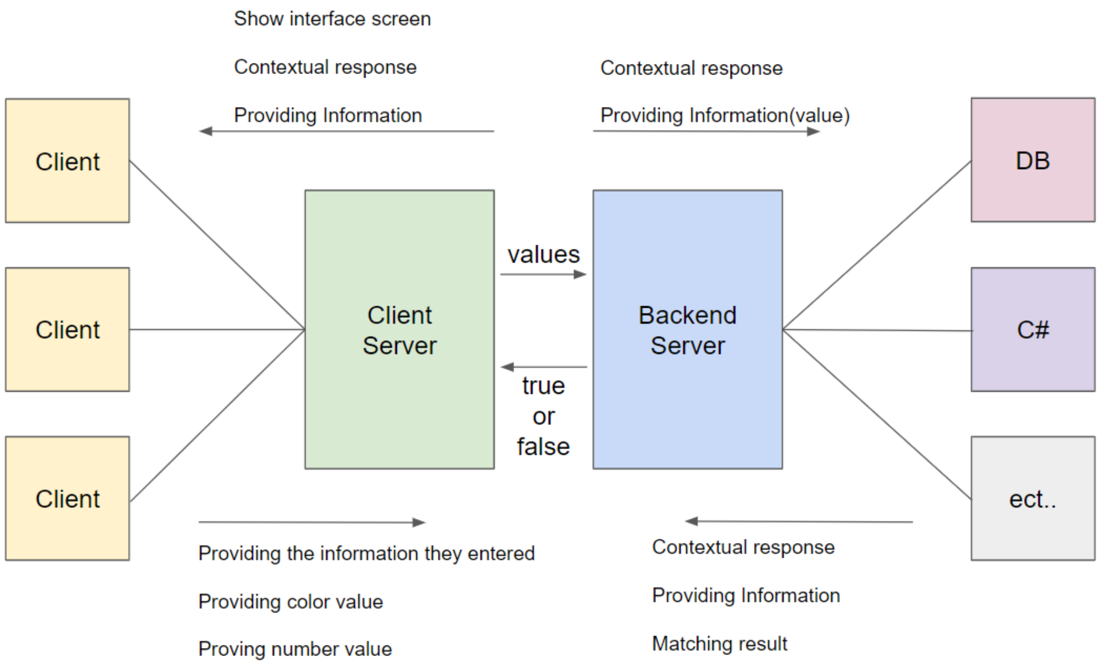
- The combination of colors, letters, and numbers will move positions separately and create a block (coordinates accordingly) every time a user enters a key.

- A user will not enter the password itself, but coordinates based on the original password set in the beginning by the user.

- This software will use SQL to strengthen database security.

Section 3 “External Interface Requirements”:

3.1 User Interfaces:



This product can be provided both in mobile and desktop(laptop) environments. Both use web interface, and can be accessed with most type of browsers:

- Chrome
- Firefox
- Microsoft Edge

3.2 Hardware Interfaces:

- A computer
- A laptop
- A cellphone
- Extra monitors
- Keyboard
- Mouse

3.3 Software Interfaces:

- A calendar: to send the date of user's log-in & out information to the server

- A timer: to set the time limitation when inputting the password

Deliverable #2

Identify the stakeholders related to your project and create a Stakeholder register

Stakeholder Register					
Stakeholder Name	Stakeholder Position	External/ Internal	Stakeholder contact details	Operational/ Executive	Interest (high, medium, low)
David Lee	Customer	External	davidL@gmail.com	Operational	High
Sophia Smith	Investor	External	sophiaS@gamail.com	Executive	High
Rose Wilson	Programmer	Internal	roseW@gmail.com	Executive	Medium
Ron Walton	Marketing officer	Internal	ronW@gmail.com	Operational	Low
Meri Cornell	End-user	External	meriC@gmail.com	Operational	Low
Erin Sheppard	Project manager	Internal	erinS@gmail.com	Executive	High
Alicia Florrick	IT administrator	Internal	AliciaF@gmail.com	Operational	High
Diane Lockhart	IT security officer	Internal	DIaneL@gmail.com	Operational	High

Deliverable #3

Prepare interview questions that you as a software engineer will ask the stakeholders. The questions should clarify issues surrounding the applications that you are developing. In order to carry out this exercise, carry out a role play within the team members where one of the team members would assume the role of a stakeholder and the rest of the team would assume the roles of the software engineering teams. Repeat the role play at least four times to gain good insight and record all questions and answers on the question template. A minimum of 5 questions per round should be recorded.

Interview Questions		
Questions	Stakeholder Position	Answer
1) Why do you need graphical password software? 2) What concerns do you have regarding the use of the product?	Customer	1) There are people who try shoulder surfing, and I want to make a new & fast software system that can prevent it. 2) It takes some time to enter a password compared to other traditional ways.
What kind of programs will you use to develop the software?	Developers & Designers	C#, JavaScript & HTML, CSS, Photoshop, Figma
1) To which continents/countries will you offer services on the software? 2) Who is the target audience?	Marketing Team	1) Across the world 2) Those who need an enhanced security system
What type of Database is used in your company?	IT Administration Team	Oracle
1) Which agile process will you use? 2) How long will it take to complete the project? 3) How many sprints will be there?	Project manager	1) Scrum 2) A month 3) Once a week (4 times)
Where will you use this product?	End-user	In public places like a café, library, subway etc.
How are you going to sell the new software?	Sales Team	A combination sale. Since it is a new and rather complicated system, we will need to sell with our other password software and leave it to the users to decide which

		password system they will use.
Will there be any conflict of interest with our other password software?	Company	No. Users will decide which password program to use. We are just offering options.
How much budget do you expect for the project?	Business Analyst	$10,000 (USD)
What made you decide to invest in this product?	Investors	We expect huge market potential related to the graphical password software.

Deliverable #4

Functional Requirements list 1:

Functional Requirements list				
Requirement ID	Requirement title	Short Description	Priority	Requester
FR01	Color Palette	The software should allow the user to select a color to enter matching letters.	High	End-User
FR02	Login API	The software must provide the API to ensure compatibility with all sites or services and successful login execution.	High	Customer
FR03	Keyboard Shortcut	The software provides keyboard shortcuts for users to shorten the password entering time.	High	End-User
FR04	Activation/Deactivation Toggle Button	The software can be deactivated when it’s unwanted to function.	Medium	End-User
FR05	Shortcut Keys Manual	Because the usage of keyboard shortcut can be tricky or difficult for some users, it provides	Medium	End-User

		a guide on how to use the shortcut.		
FR06	Language Setting	The software provides various language preferences for global users.	Medium	End-User
FR07	Color Lightness/Contrast Controller	The software allows users to set the lightness or contrast of the selected color for stronger security when signing in.	Low	End-User
FR08	Chatbot Service	The software provides AI Chatbot service to answer users' instant questions.	Low	End-User
FR09	Color Preference Personalization	The software collects each user's frequently used color and lets the system save it, so that the user can immediately bring the frequently used color.	Low	Programmer
FR10	Security Alert	The software shows a pop-up alert when the user tries to login using shared network, or when the software detects virus.	Low	End-User

Non-functional Requirements list 2:

Nonfunctional Requirements list				
Requirement ID	Requirement title	Short Description	Priority	Requester
NFR01	Cyber Security	The system should pass the following tests: DDoS testing, penetration testing and malicious script testing.	High	IT security officer
NFR02	Performance	The landing page supporting ten thousand users per hour must provide 3 seconds or less response time in a Chrome desktop browser, including the rendering of text and images, over an LTE connection.	High	IT administrator
NFR03	Availiability	The web must be available to users 97 percent of the time every month	High	IT administrator
NFR04	Reliability Warning Messages	The system should produce a “system warning” message when the capacity of service requests reached above 70%, and additional warning message at 5% request increments.	Low	IT administrator
NFR05	Web Browser Compatibility	The new system should be compatible with the following browsers: Chrome, Firefox and Microsoft Edge, and Safari.	Medium	IT administrator
NFR06	Mobile Compatibility	The new system should be compatible with	Medium	IT administrator

		the following mobiles: IOS, Android		
NFR07	Localization – Format	The graphical password system will support HSLA color values, and QUERTY type keyboards	Medium	IT administrator
NFR08	Usability	The error rate of users entering their passwords at the landing page must not exceed 5 percent.	High	IT administrator
NFR09	Security	For the purpose of enhanced security, notify user of message of requiring change of color on a regular basis.(rather than frequent change of numbering passwords, simply changing a color come in handy).	High	IT security officer

Summer 2022

COMP 225 (SEC 006)

Team Project B

Group 8:

Jungyu Lee,

Manvibolreach Ouk

Centennial College

Inqulab Ahir

July 17, 2022

Assignment #2 (Part B)

Group 8: Jungyu Lee, Manvibolreach Ouk

Deliverable #1

Based on the list of requirements you gathered in Part A of the project, develop a set of goal use cases per use case identify the actors (Operational stakeholders) involved and the requirements they relate to. Name each use case to reflect the functionality it serves using the name convention “Verb-Noun” group the uses cases under two or three sub-systems / modules. You can base your grouping based on the similar functional areas or based on types of operational stakeholders, who are your end users.

Add the use case table to section # 3 of your SRS document.

Use Cases			
Use Case name	**List of related Requirements ID**	**Actor(s)**	**Brief Description**
Select color from palette	FR01	- All service users including mobile banking users, students, teachers, senior citizens - IT administrators	All service users will choose a specific color from the palette to set up the passwords at the beginning of the system. They will enter the passwords which will match the coordinates. This process is required for all service users to use the graphical password system. While the customer can choose colors from the palette, the color will be given as HSLA values to the IT administrators.
Log-in to the system	FR02	- All service users including mobile banking users, students, teachers, senior citizens - IT administrators - Programmers	Log-in API is one of the most fundamental functions in the system. Therefore, it is required for all service users to use this system. Log-in API is connected with the graphical password software and allows the service users to enter user’s information including the passwords. IT administrators will do the usual work to run the login API, and programmers will do the maintenance work if necessary.
Use keyboard shortcuts	FR03, FR05	All service users including mobile banking users, students, teachers, senior citizens	All service users will use keyboard shortcuts to enter the passwords. This is the core function in the graphical password system. A user will set their passwords combined with colors, letters, and numbers. Every time the user tries to

		- IT security officers	enter the passwords, the graphical passwords software will offer random coordinates for passwords. The user can press keyboard shortcuts which are mapped with each coordinate. The user can customize his/her own shortcut key as well as simply using the default shortcut key. The algorithms for random coordinates must not be predictable and maintained regularly to provide the stable password security by IT security officers.
Turn on/off button	FR04	All service users including mobile banking users, students, teachers, senior citizens	The graphical passwords system is optional, which means all service users can deactivate it, and use the traditional passwords system with the turn on/off button when necessary. Users can find this button at the top right of the corner of the screen. If they turn the button off, the system will disappear and provide traditional passwords log-in API. When they turn the button on, the system will show up and work again.
Change language settings	FR06, FR08	- All service users including mobile banking users, students, teachers, senior citizens - IT administrators	All service users can change the language preferable to them. The graphical passwords software will present several languages such as English, Spanish, Arabic, et cetera. The users will select the preferred language. The software will automatically change the language for the manual, chatbot service, and guidelines, which will be managed and updated by IT administrators.
Choose preferred color options	FR07	- All service users including mobile banking users, students, teachers, senior citizens	All service users can set colors to their taste. They will click on the color option button. This function is going to be popular especially for the younger generation since it can show individuality. Furthermore, based on their selected colors, the colors will take turns every time the actor tries to log in, which will help enhance security.

Talk to Chatbot	FR08	- All service users including mobile banking users, students, teachers, senior citizens - IT administrators	All service users can use chatbot service when they encounter problems. They will click on the chatbot service button. This chatbot service is based on AI, so users can get instant answers to their questions. In addition, for senior citizens who prefer talk to type, the chatbot can recognize users' voices and produce answers. The users can not only see the message produced, but also can hear AI's voice. The chatbot system will be maintained by IT administrator.
Bring colors back	FR09, FR07	- All service users including mobile banking users, students, teachers, senior citizens - IT administrators	Since the software utilizes HSLA values for colors, it is hard for users to remember the exact value. A user can make a list of their preferred colors. Also, the user can delete colors which are no longer used from the list or add colors to the list. Even if the list has no colors previously used by users, there is a color history. The user can ask IT administrators to bring back colors. IT administrators can access the history of users and add the colors to the user's list.
Send warning messages	FR10	- All service users including mobile banking users, students, teachers, senior citizens - IT security officers	When a user clicks on the log in button using shared Wi-Fi or networks, the software automatically sends messages whether to proceed. Furthermore, when the software detects viruses or potential danger, the software sends warning messages to the users to shut off the software. When the warning message is sent, the system will automatically alert IT security officers to monitor the system.

Deliverable #2

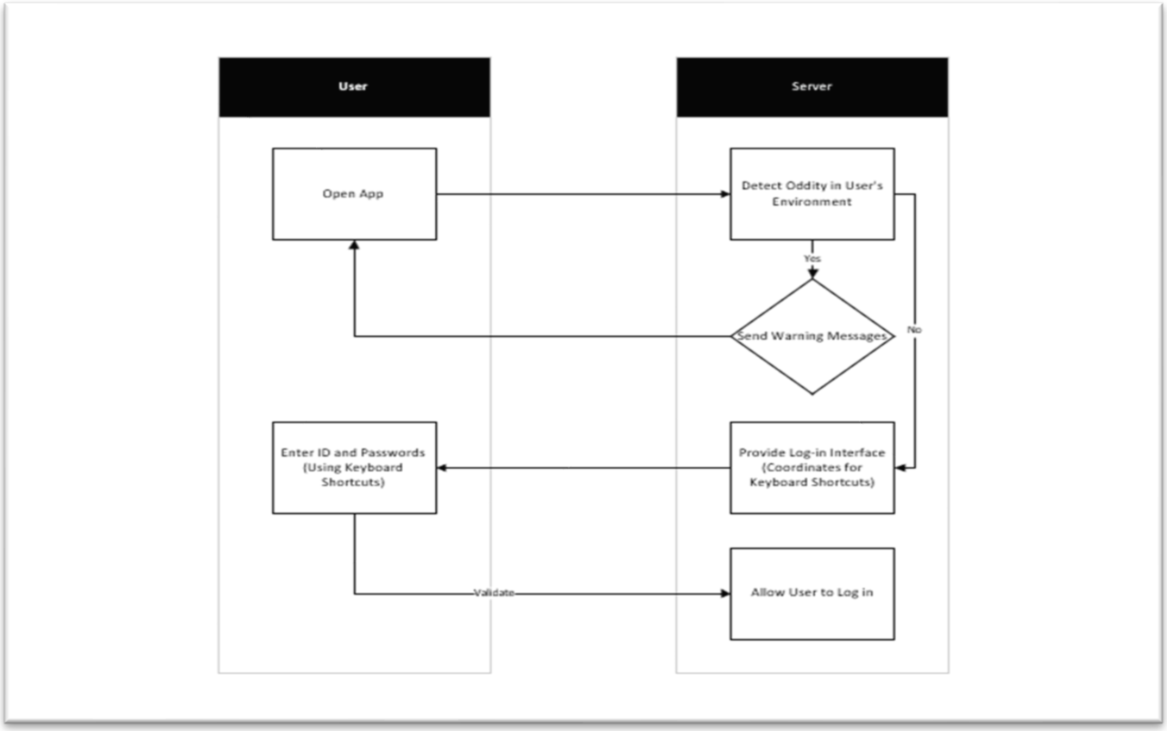
Select one use case with high priority and develop a textual detailed formal use case description, using the use case template in chapter #8 page 136. Supplement the use case with a swim lane activity diagram, explaining the flow of activities between the system and the actor(s).

Add the use-case formal descriptions and the activity swim lane diagrams to section #4 of your SRS document.

Textual Detailed Formal Use Case Description	
Use case	Use keyboard shortcut
Iteration	1, last modification: June 16, 2022
Primary actor	Mobile banking user
Goal in context	To enter passwords safely at a faster speed
Preconditions	The system must be fully configured. Initial passwords (a combination of colors, numbers, and letters) must be set by a user. Algorithms must be active to provide coordinates for passwords.
Trigger	The mobile banking user enters ID. The system recognizes the user's passwords matching the ID and provide the coordinates for passwords.
Scenario	1. The mobile banking user (the user) opens the banking app. 2. The user enters ID, and the server checks the ID. 3. The user is given the map for random colors, letters, and numbers from the server. 4. The user enters color coordinates that correspond the specific position on the map by using keyboard shortcuts. 5. The user enters letter coordinates that correspond the specific position on the map by using keyboard shortcuts. 6. The user enters number coordinates that correspond the specific position on the map by using keyboard shortcuts. 7. The user enters all the passwords and click on the log-in button. 8. The complete coordinates mapping with the user's passwords are delivered to the server. 9. The user logs in to the banking system successfully.
Exceptions	- The server detects shared networks or viruses on user's part. It sends warning messages to the user whether to proceed. - ID is incorrect. The user has to go through ID validation process. - Passwords are incorrect. The user is given three different maps to try, then has to go through passwords validation process. - The user can traditional password log-in system with turn on/off button – See Use Case Turn on/off button.
Priority	Highest - the core of the graphical password system
When available	Third Increment

Frequency of use	High.
Channel to actor	Via PC-based browser, mobile-based browser, mobile application with Internet connection.
Secondary actors	- Server - IT security officers
Channels to secondary actors	Via PC-based browser, mobile-based browser, mobile application with Internet connection.
Open issues	- Is security sufficient? Hacking into the feature would represent a major invasion of privacy. - What mechanisms trigger the warning message system to protect the user? - How algorithms provide maps for coordinates, and is it enough and well-functioned?

Swim Lane Activity Diagram

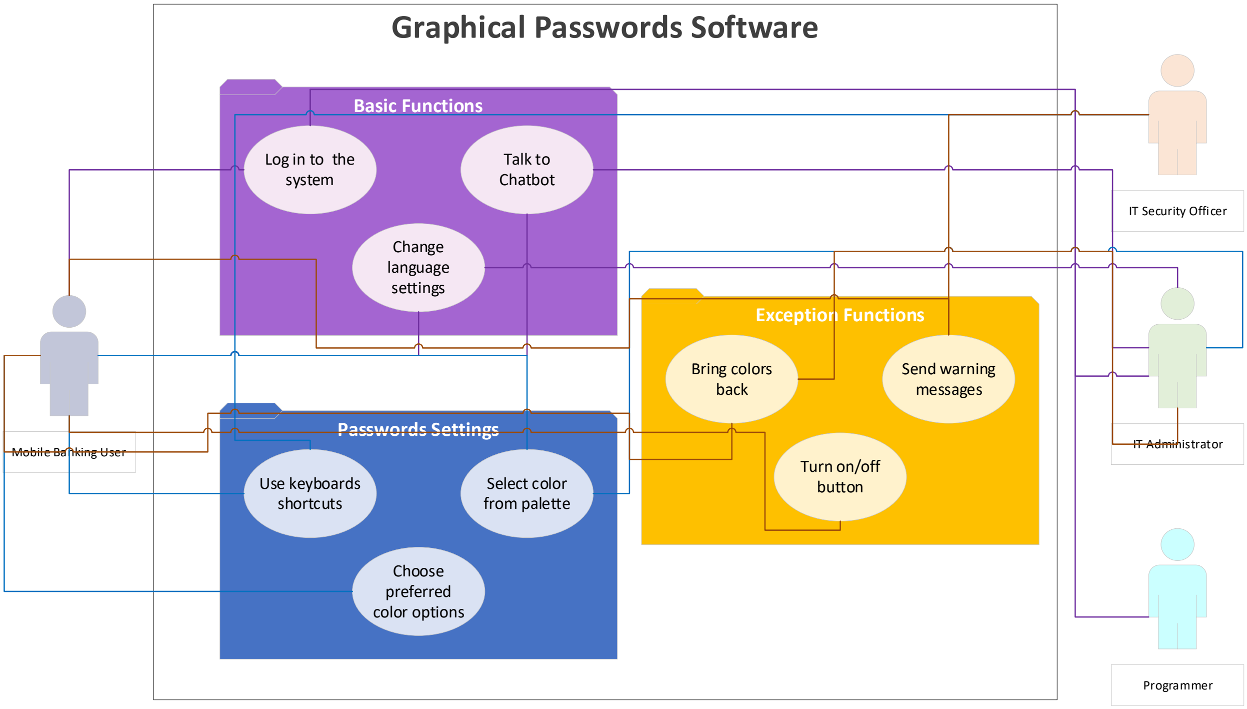

User
Server
Open App
Detect Oddity in User's Environment
Yes
Send Warning Messages
No
Enter ID and Passwords (Using Keyboard Shortcuts)
Provide Log-in Interface (Coordinates for Keyboard Shortcuts)
Validate
Allow User to Log in

Deliverable #3

Using "Microsoft Visio" draw a use case diagram illustrating all the use cases identified in deliverable 1 above grouped by sub-system.

Add the output to section #4 of your SRS document.

Use Case Diagram



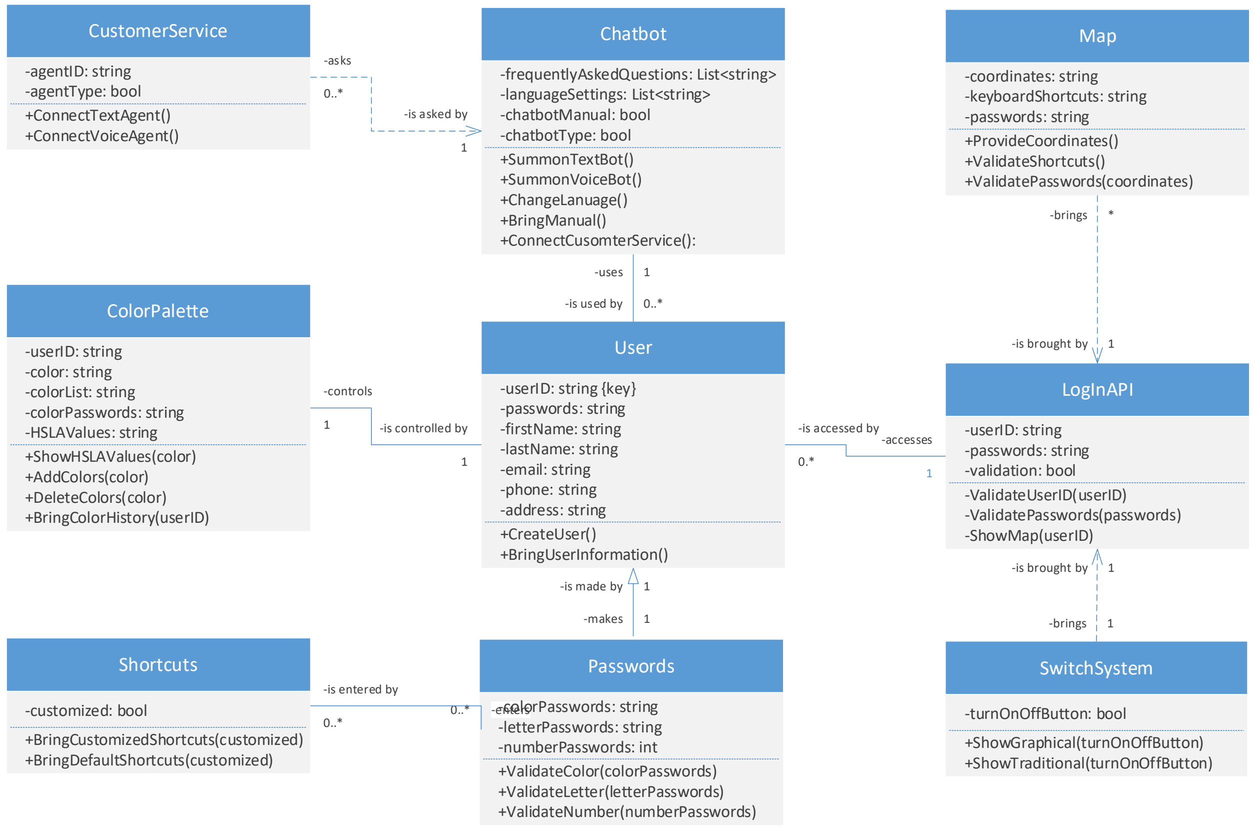
Deliverable #4

Based on the use case descriptions, use the “Noun” technique to identify a list of analysis classes related to the domain problem/opportunity of your project. Brainstorm with your team to identify the list of attributes related to each class and the class relationships, for example binary association, inheritance…etc. and describe these relationships, for example a customer places an order, an order belongs to one customer. Draw, using “Microsoft Visio” a first cut domain class diagram.

Add the domain class diagram.

Domain Class Diagram

Graphical Passwords Software



Deliverable #5

Brainstorm with your team to develop a set of Class responsibilities and collaboration “CRC cards” for all entity type classes.

Add the CRC index cards.

CRC Index Cards

User

Responsibilities	Collaborators
create a new user bring user information	LogInAPI ColorPalette Passwords Chatbot Shortcuts

Attributes

userID: string
passwords: string
firstName: string
lastName: string
email: string
phone: string
address: string

LogInAPI

Responsibilities	Collaborators
validate user ID validate passwords show map	User SwitchSystem Map

Attributes

userID: string
passwords: string
validation: bool

Passwords

Responsibilities	Collaborators
validate color passwords validate letter passwords validate number passwords	User ColorPalette Shortcuts

Attributes

colorPasswords: string
letterPasswords: string
numberPasswords: int

ColorPalette

Responsibilities	Collaborators
show HSLA values add colors to the list delete colors from the list bring user's color history	User Passwords

Attributes

userID: string
color: string
colorList: string
colorPasswords: string
HSLAValues: string

Chatbot

Responsibilities	Collaborators
summon text chatbot summon voice chatbot change language settings bring chatbot manual connect to customer service	User CustomerService

Attributes

frequentlyAskedQuestions: List<string>
languageSetings: List<string>
chatbotManual: bool
chatbotType: bool

Customer Service

Responsibilities	Collaborators
connect to text agent connect to voice agent	Chatbot

Attributes

agentID: string
agentType: bool

Map

Responsibilities	Collaborators
provide coordinates validate shortcuts validate passwords	LogInAPI Shortcuts

Attributes

coordinates: string
keyboardShortcuts: string
passwords: string

SwitchSystem

Responsibilities	Collaborators
show graphical system	LogInAPI
show traditional system	

Attributes

turnOnOffButton: bool

Shortcuts

Responsibilities	Collaborators
bring customized shortcuts	Passwords
bring default shortcuts	User

Attributes

customized: bool

Deliverable #6 Based on the responsibilities and collaborations identified in your CRC index cards update your first cut domain class diagram with the following:

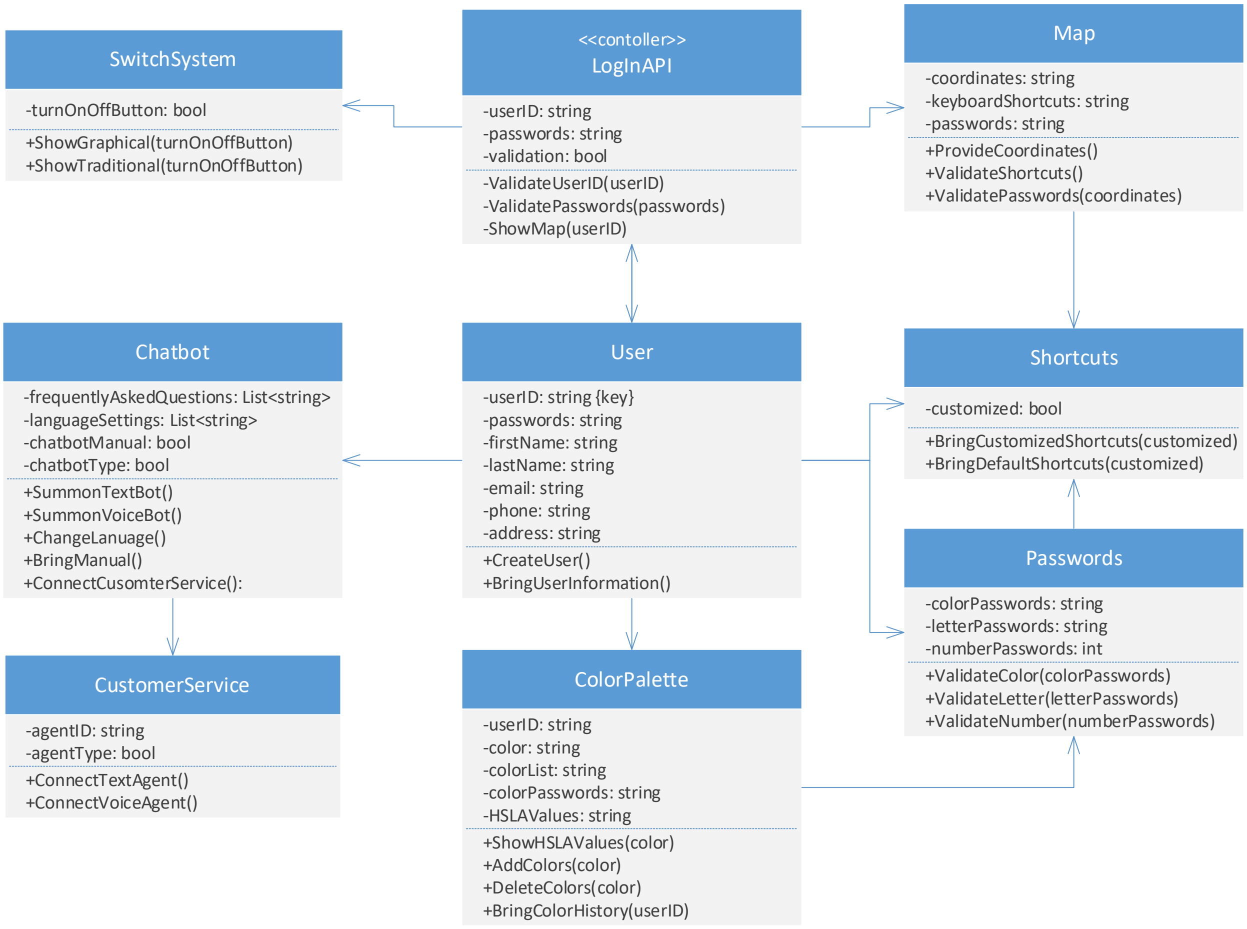
a. Class attribute descriptions and visibilities

b. Signature methods with the respective parameters and visibilities

Add the class diagram to Appendix E of your SRS document under class diagrams.

Updated First Cut Domain Class

Graphical Passwords Software



Summer 2022

COMP 225 (SEC 006)

Team Project C

Group 8:

Jungyu Lee,

Manvibolreach Ouk

Centennial College

Inqulab Ahir

August, 2022

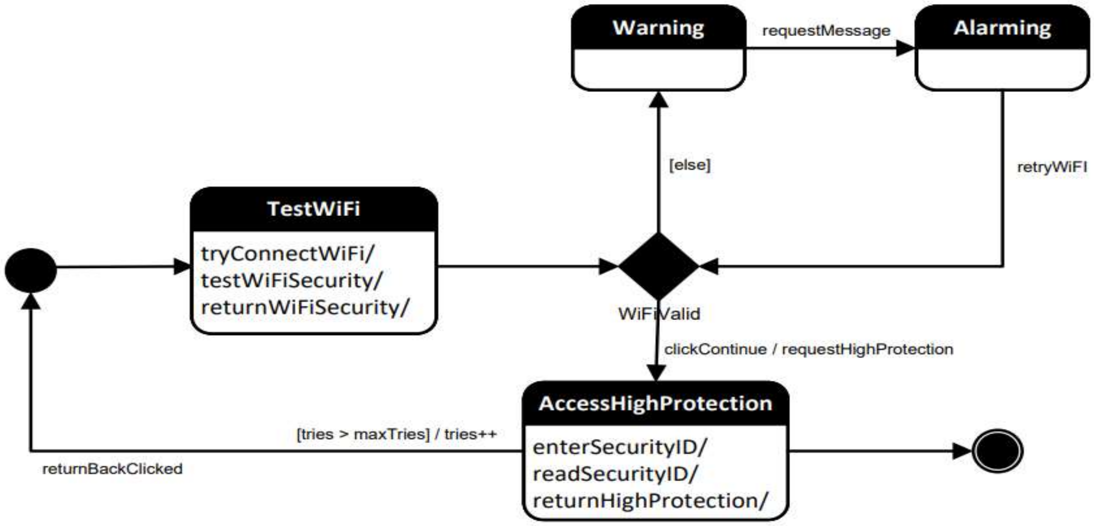
Assignment #3 (Part C)

Group 8: Jungyu Lee, Manvibolreach Ouk

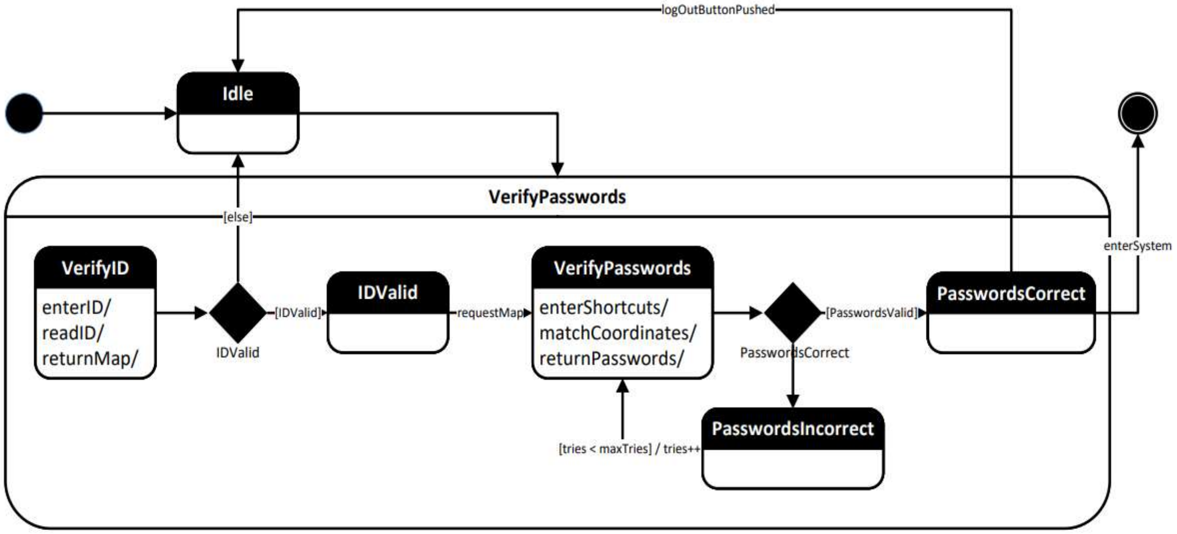
Deliverable #1

Select two entity classes from deliverable #3 "Part B" and develop two state diagrams. The classes should have a dynamic nature within the scope of your project. Add the state diagrams to Appendix E of your SRS document.

State Machine Diagram #1 – Send Warning Messages



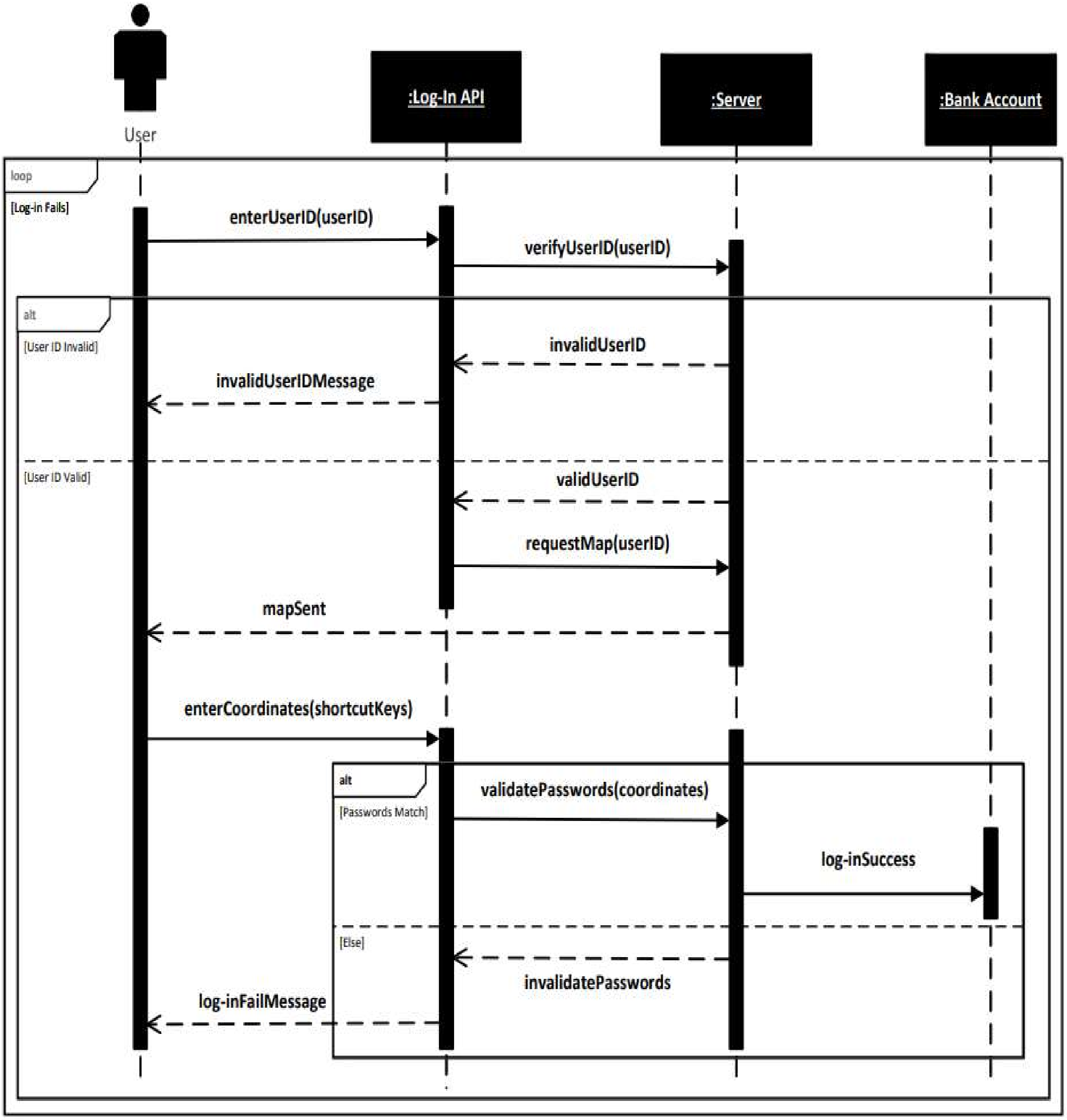
State Machine Diagram #2 – Use Keyboard Shortcuts



Deliverable #2

Based on the formal use case description you created in deliverable #2 in Part B, develop a sequence diagram using Microsoft Visio. Add the sequence diagram to Appendix E of your SRS document.

Sequence Diagram – Use Keyboard Shortcuts



Deliverable #3

Carryout a simple technical review for another teams Part A & Part B project as agreed with your Professor in week#10, review the specification in terms of the below requirements quality attributes:

Technical Review On Group 5

Attributes	Metric
1. Ambiguity	There is no number of weak phrases and number of optional phrases.
2. Completeness	The number of To Be Determined (TBDs): Completed The number of To Be Added (TBAs): Completed
3. Understandability	The material in the document is readable, and the document's structure is in order and corresponds to the examples.
4. Volatility	There are a few numbers of changes per requirement time (by activity) when change is requested.
5. Traceability	There are many numbers of requirements not traceable to design/code and testing.
6. Model Clarity	There are 7 UML models. There is at least 1 descriptive page per UML model. The number of UML errors is not found in the document.

Write a free text of your findings against each of the six attributes. Discuss with your professor and submit the quality report in the assessment folder week #13 indicating which another team (Project name and Group#1) your team reviewed.

The document, which is a good solution to the issue of the inconvenience of borrowing books from the library, is supported by a solid timeframe and a long-term aim of community members. The document is full and meets all software requirements; there are no missing pieces. And the cause of volatility has been linked to a shift in circumstance brought on by the global viral outbreak.

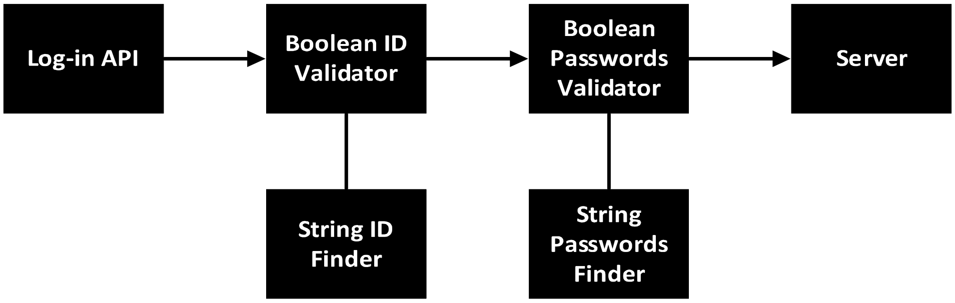
A useful research topic for creating an app to assist students in using library materials in this period is Covid 19. It is clear that using an app to check out books from the library is a common practice in today's society even though the virus outbreak has been lower than it was before.

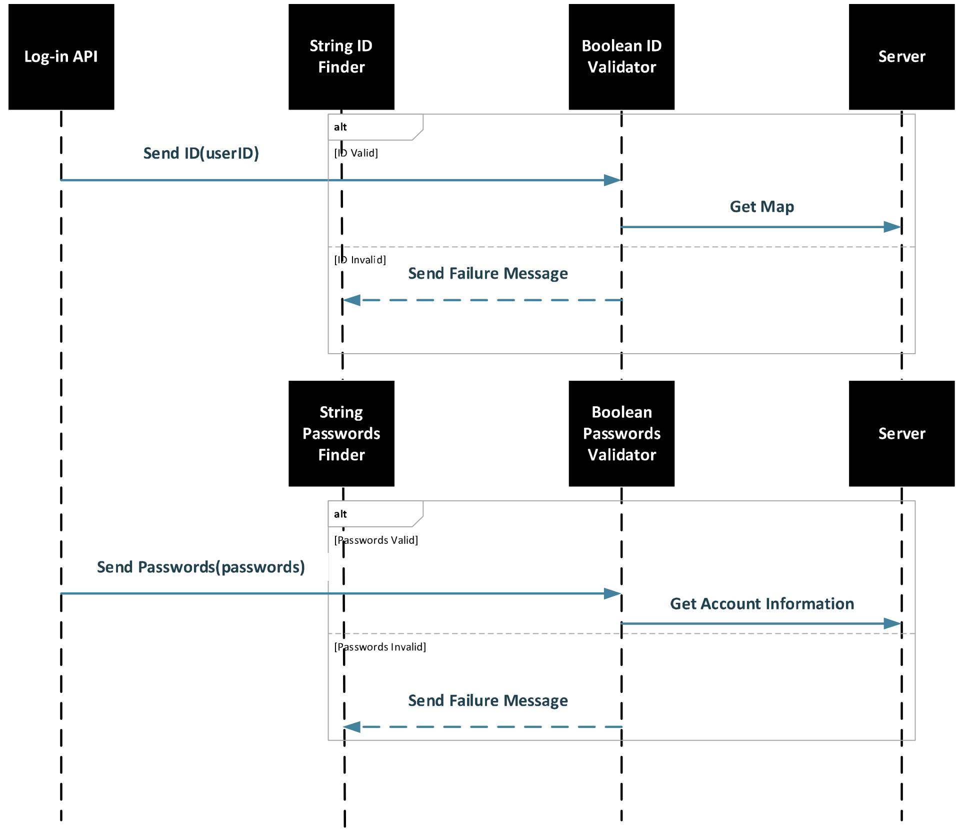
However, in traceability parts, the app cannot yet be built using simply C#. Before the developers choose the technology or programming languages for creating the product, more programming languages are required, and the system must be built with UI and UX design. Requires cyber security technologies to safeguard the software as specified in the document. The paper is missing software actors who would be unable to work as a team, as well as testers. To handle the entire software, the team would require at least two designers and four to five coders.

Deliverable #4

Research the "Party Analysis pattern" investigate the possibility of updating your class diagram using this analysis pattern. If possible, add the updated class diagram to Appendix E under class diagrams. Write a small paragraph explaining the value of using this pattern within the context of your project. If not possible write a paragraph stating, why this pattern cannot be used in the context of your project.

Analysis Pattern

1. Pattern Name	Recover Forgotten ID and Passwords
2. Intent	Specify the procedure of recovering forgotten ID and passwords.
3. Motivation	The Recovering ID & Passwords pattern is deeply interconnected with the log in process. When a user fails to enter proper ID or passwords, the log-in API will give the user another chance to enter ID or passwords. Also, the log-in API will show both Forgot ID? and Forgot Passwords? buttons so that the user can recover the ID and passwords. The server has the user's information, such as email and phone number, so the server can validate user's identity.
4. Constraints	- The server has a valid user's email and phone number. - The user has to remember the email and phone number information at the time he or she registered.
5. Applicability	This process will be applicable to all users who use the graphical passwords software.
6. Structure	 Log-in API Boolean ID Validator Boolean Passwords Validator Server String ID Finder String Passwords Finder

7. Behavior	 Log-in API String ID Finder Boolean ID Validator Server alt [ID Valid] Send ID(userID) Get Map [ID Invalid] Send Failure Message String Passwords Finder Boolean Passwords Validator Server alt [Passwords Valid] Send Passwords(passwords) Get Account Information [Passwords Invalid] Send Failure Message
8. Participants	- Log-in API: Defines the UI that the user can enter ID and passwords into. - BooleanIDValidator: Defines whether the entered ID is true or false. - StringIDFinder: Defines the information the user receives when ID is forgotten. - BooleanPasswordsValidator: Defines whether the entered passwords are true or false. - StringPasswordsFinder: Defines the information the user receives when passwords are forgotten. - Server: Defines the whole log-in process.
9. Collaborations	- Since the pattern is a part of log-in process, it interacts with the Log-in API. - When BooleanIDValidator or BooleanPasswordsValidator fails, StringIDFinder or StringPasswordsFinder gets active.
10. Consequences	- Validators and Finders have a common interface. - Complicated Log-in processes are integrated into one process.

Deliverable #5

Prepare a power point presentation, using the template posted on the course shell, to be presented end of term.

The PowerPoint slides for deliverable #5 are separately attached.