Project Report

ON

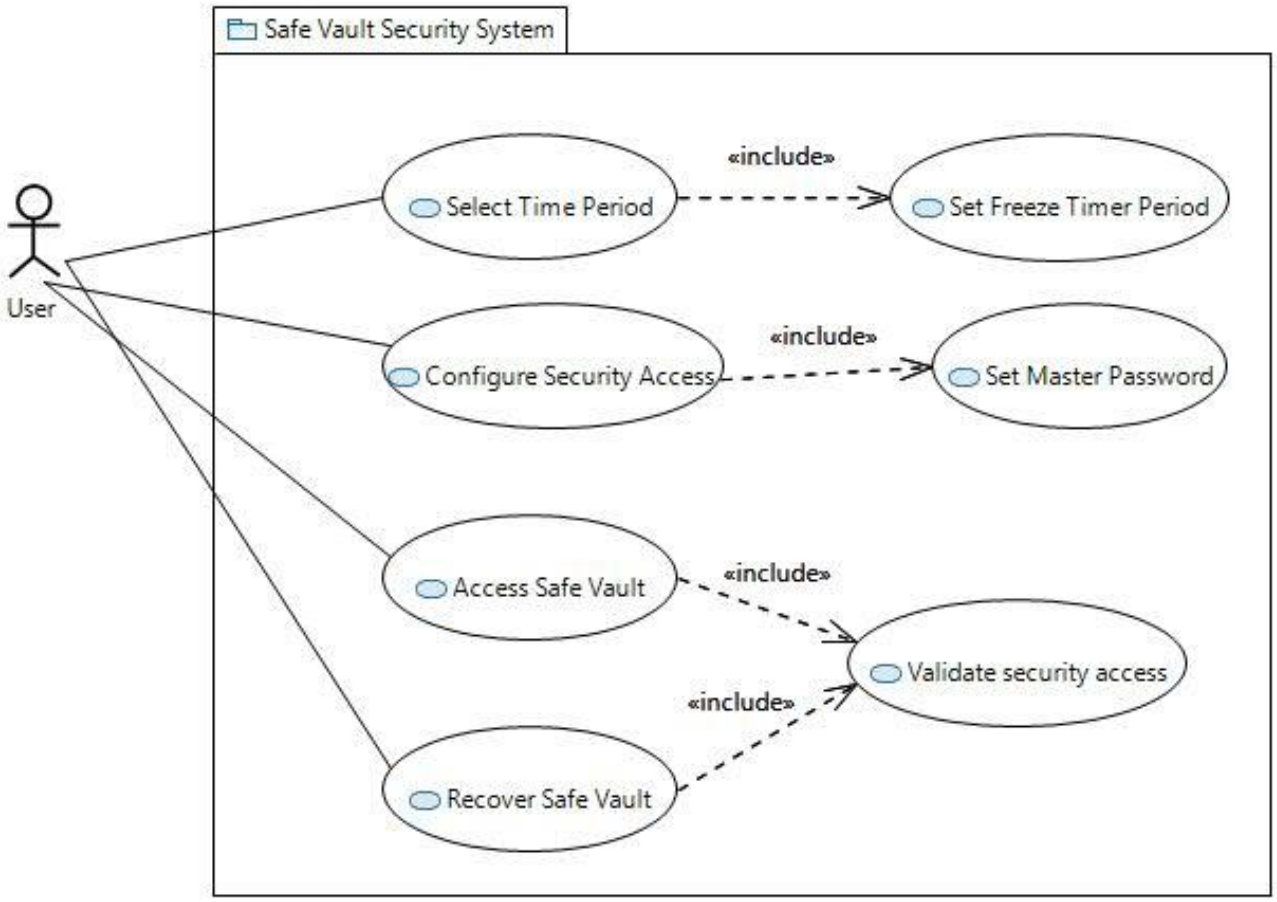
Timer Based Security System for Safe Vaults
Using COMET Methodology

Problem Statement:

- Timer based security system is a type of security system of single person use in which the vault can be accessed only when a particular times of the day are reached.
- The particular times of the day are decided by the user himself beforehand.
- When the particular time is reached, the user has to clear six security levels each of ten seconds which is totally sixty seconds covering an entire minute.
- The six security levels can be of any security implementation like voice recognition, thumb print scanning, Retina scanning, answering a security question, identifying an image among set of images, drawing a preconfigured pattern. A pattern is the one which is generated by joining dots with lines. Drawing pattern is one of the common security access methods in android phones.
- If the user failed to clear any one of the gate level, then the user will be requested to clear a master security password within five seconds which returns the user to the current security level.
- If all the security levels have been successfully cleared then the user will be permitted to access the safe vault.
- If the master password is wrong or any security level is not cleared, then the entire system freezes for specified amount of time (which is also determined beforehand) and the system is recovered after the expiry of freeze time.
- This system can be used as a security system for the safety vaults and for securing system access containing sensitive data.

Requirements Model:

Use Case Diagram:



Validate Security Access Use Case:

Use Case Name - Validate Security Access

Summary – Validates Security Access for accessing vault

Actor – Safe Vault User

Preconditions: Safe Vault is Idle.

Description:

1. User Chooses Access Vault Option.
2. System checks for time period validity.
3. If the time is valid, then the system asks confirmation to begin validation.
4. User confirms validation
5. System Prompts for finger print validation.
6. If finger print validation successful, then the system prompts for Retina Validation.
7. If Retina scan is successful, then the system prompts for Voice Recognition.
8. If Voice Recognition is successful, then the system prompts for pattern validation.
9. If pattern validation is successful, then the system prompts for Image validation.
10. If Image validation is successful, then the system prompts for Security question validation.
11. If security question validation is successful, then the system access is granted.

Alternatives:

1. If time period is not valid, then the access is denied.
2. If any one of the validation fails, then the system prompts for master password validation.
3. If the master password validation fails, then the system is freezed for the specified amount of time.

Post condition: Vault access is granted.

Configure Security Access Use Case:

Use Case Name - Configure Security Access

Summary – Configures Security Access methods for protecting vault

Actor – Safe Vault User

Preconditions: Safe Vault is Idle.

Description:

1. User Chooses Configure security Option.
2. System checks for time period validity.
3. If the time is valid, then the system asks confirmation to begin configuration

4. User confirms initiating Configuration
5. System asks for configuration password
6. User Inputs configuration password.
7. If the configuration password is correct, System Prompts for finger print configuration.
8. If finger print configuration is successful, then the system prompts for Retina configuration.
9. If Retina Scan configuration is successful, then the system prompts for Voice configuration.
10. If Voice configuration is successful, then the system prompts for pattern configuration.
11. If pattern configuration is successful, then the system prompts for Image configuration.
12. If Image configuration is successful, then the system prompts for Security question configuration.
13. If security question configuration is successful, then the system prompts for master password configuration.
14. If master password configuration is successful, then the system access methods are configured successfully.

Alternatives:

1. If time period is not valid, then the access is denied for configuring security access.
2. If configuration password is wrong, then the access is denied for configuring security access.
3. If any one of the configuration fails, then the system configuration is not complete.

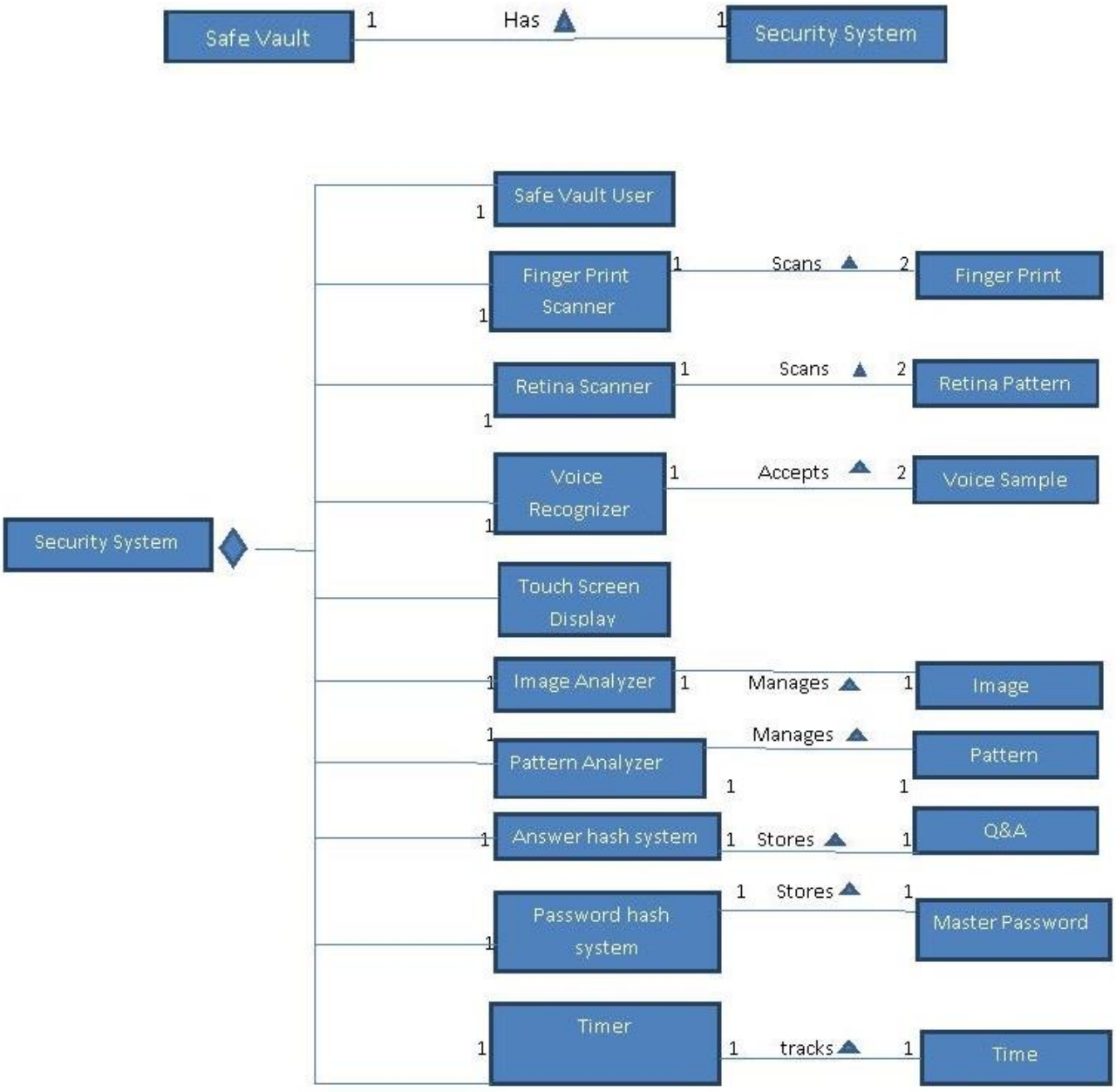
Post condition: Configuration of access method is completed.

Analysis Model:

Analysis Static Model:

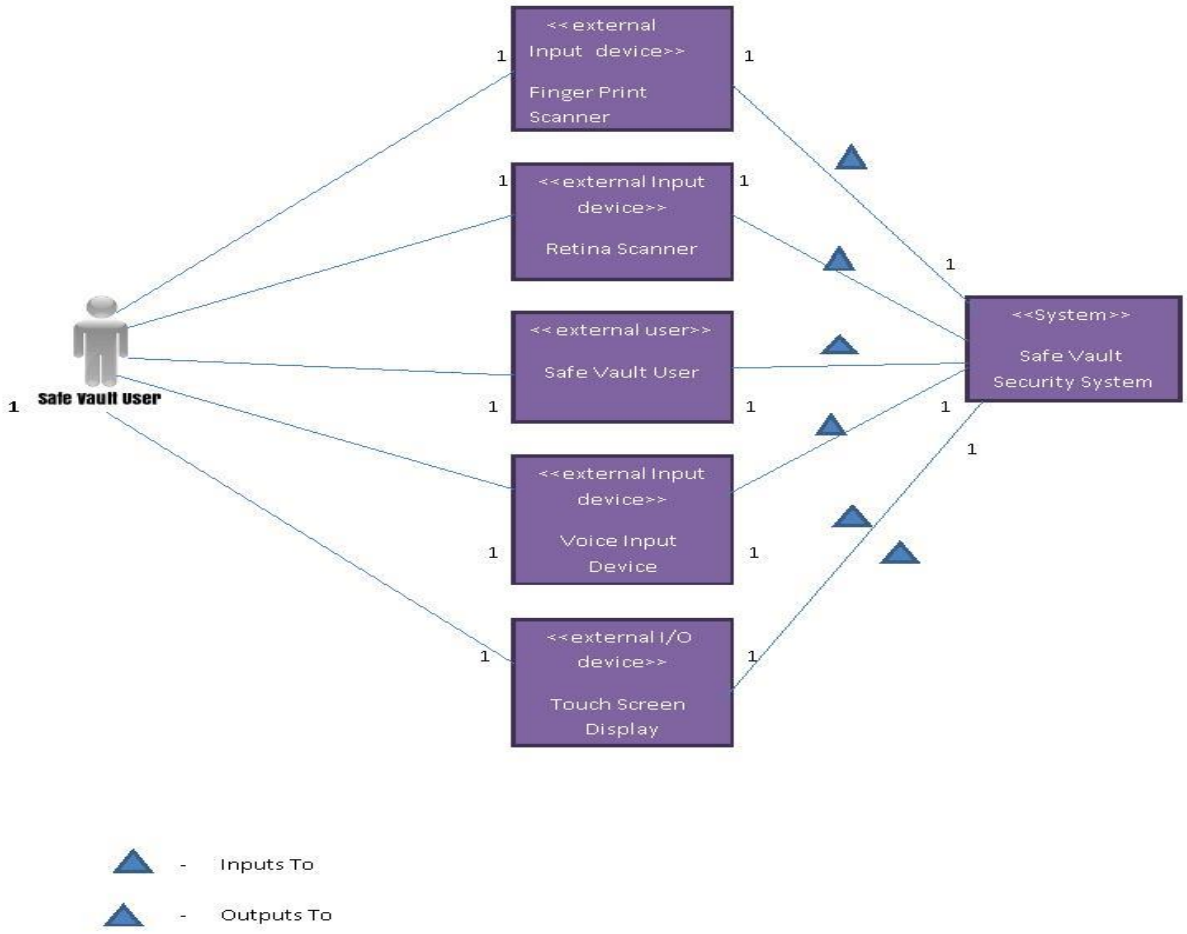
Identifying physical Objects:

The physical objects are safe vault, security system, safe vault user, finger print scanner device, retina scanner device, voice recognizer and user touch screen display and etc. The corresponding class diagram is as follows.


Safe Vault
1
Has
1
Security System
Security System
Safe Vault User
1
Finger Print Scanner
1
1
Scans
2
Finger Print
Retina Scanner
1
1
Scans
2
Retina Pattern
Voice Recognizer
1
1
Accepts
2
Voice Sample
Touch Screen Display
Image Analyzer
1
1
Manages
1
Image
Pattern Analyzer
1
1
Manages
1
1
Pattern
Answer hash system
1
1
Stores
1
Q&A
Password hash system
1
1
Stores
1
Master Password
Timer
1
1
tracks
1
Time

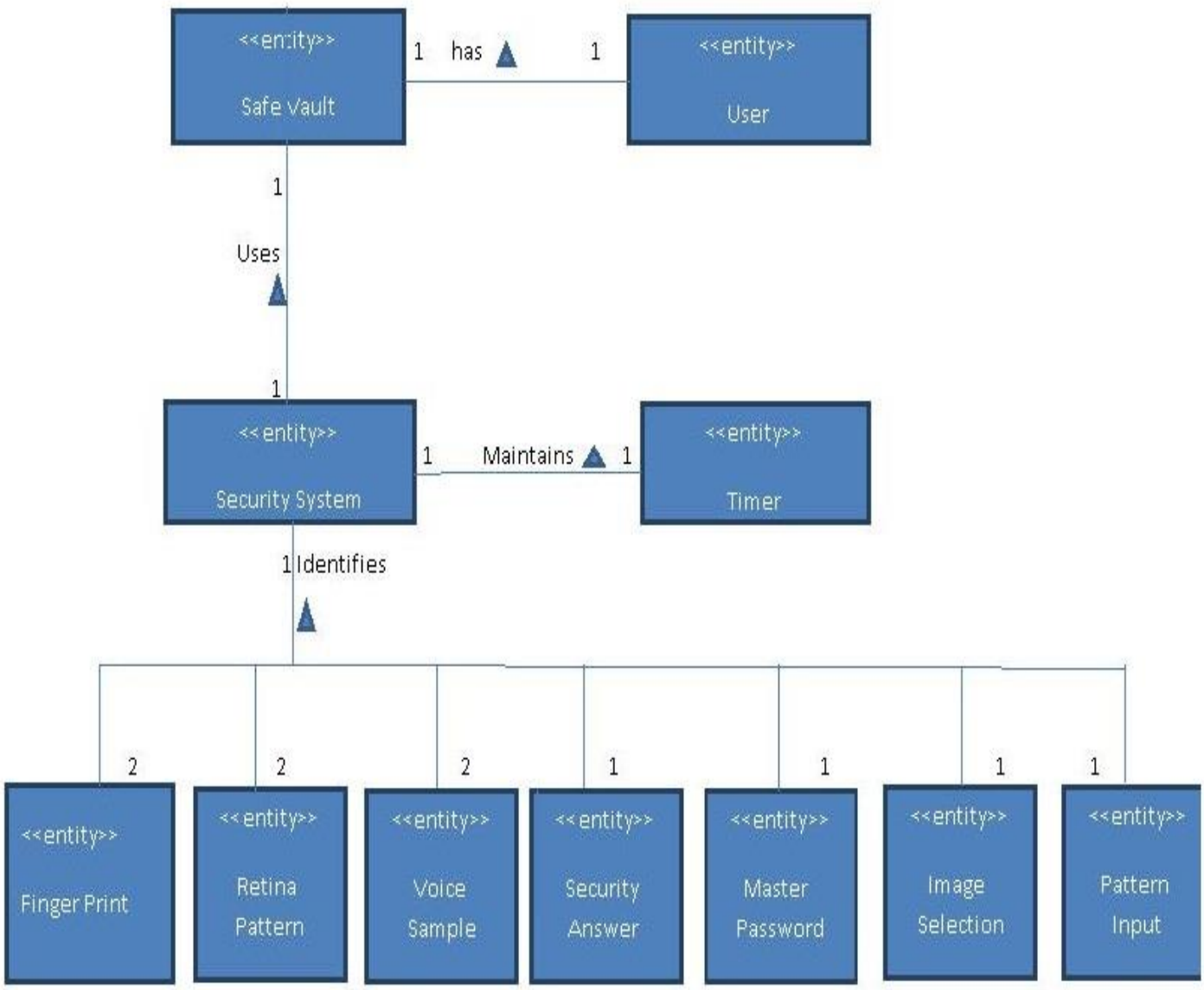
System Context Diagram:

The system context diagram is as follows.



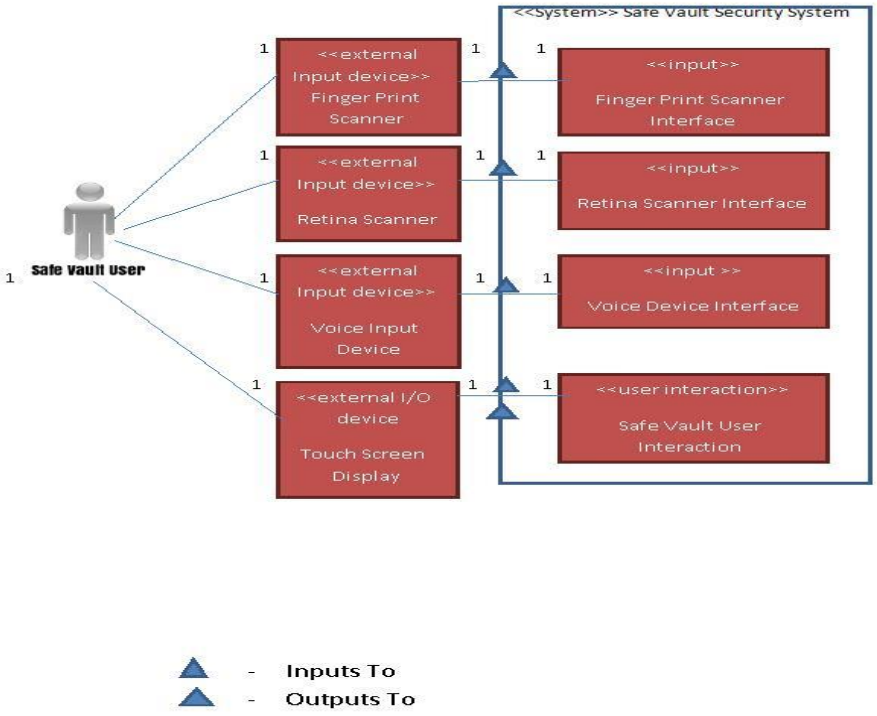
Entity Class

The following diagram shows the identified entity class for proposed system.



System Context Diagram with boundary objects:

The following diagram shows the system context diagram with the identified boundary objects for the system which forms the interface to the system.



- Inputs To
- Outputs To

Grouping Classes into subsystems:

The finger print scanner, touch screen display, security control, finger print analyzer and storage unit for finger prints forms a finger print subsystem. The analyzer and storage unit of finger print subsystem are discussed in the design phase. The retina scanner, touch screen display, security control, retina pattern analyzer and retina pattern storage unit forms a retina pattern subsystem. The analyzer and storage unit of retina subsystem are discussed in the design phase. The voice input device, touch screen display, security control, voice sample analyzer and voice storage unit forms a voice recognizer subsystem. The analyzer and storage unit of voice recognizer subsystem are discussed in the design phase. The touch screen display, security control, pattern analyzer and pattern storage unit forms a pattern processing subsystem. The pattern is any user drawn lines by connecting dots to form an arbitrary image. The touch screen display, security control, image analyzer and image storage unit forms a image processing subsystem. The touch screen display, security control, security Q&A Analyzer and the storage unit forms a security question processing subsystem often referred to Answer phrase hash system in the sequence diagrams as the details are hashed and stored in the file system. The touch screen display, security control, password analyzer and storage unit forms a password processing subsystem. It is referred as password hash system in sequence diagram as password is usually hashed and stored in the file system. The password subsystem stores and process the master password and configuration password. Thus there are seven subsystems for the proposed system.

Analysis Dynamic Model:

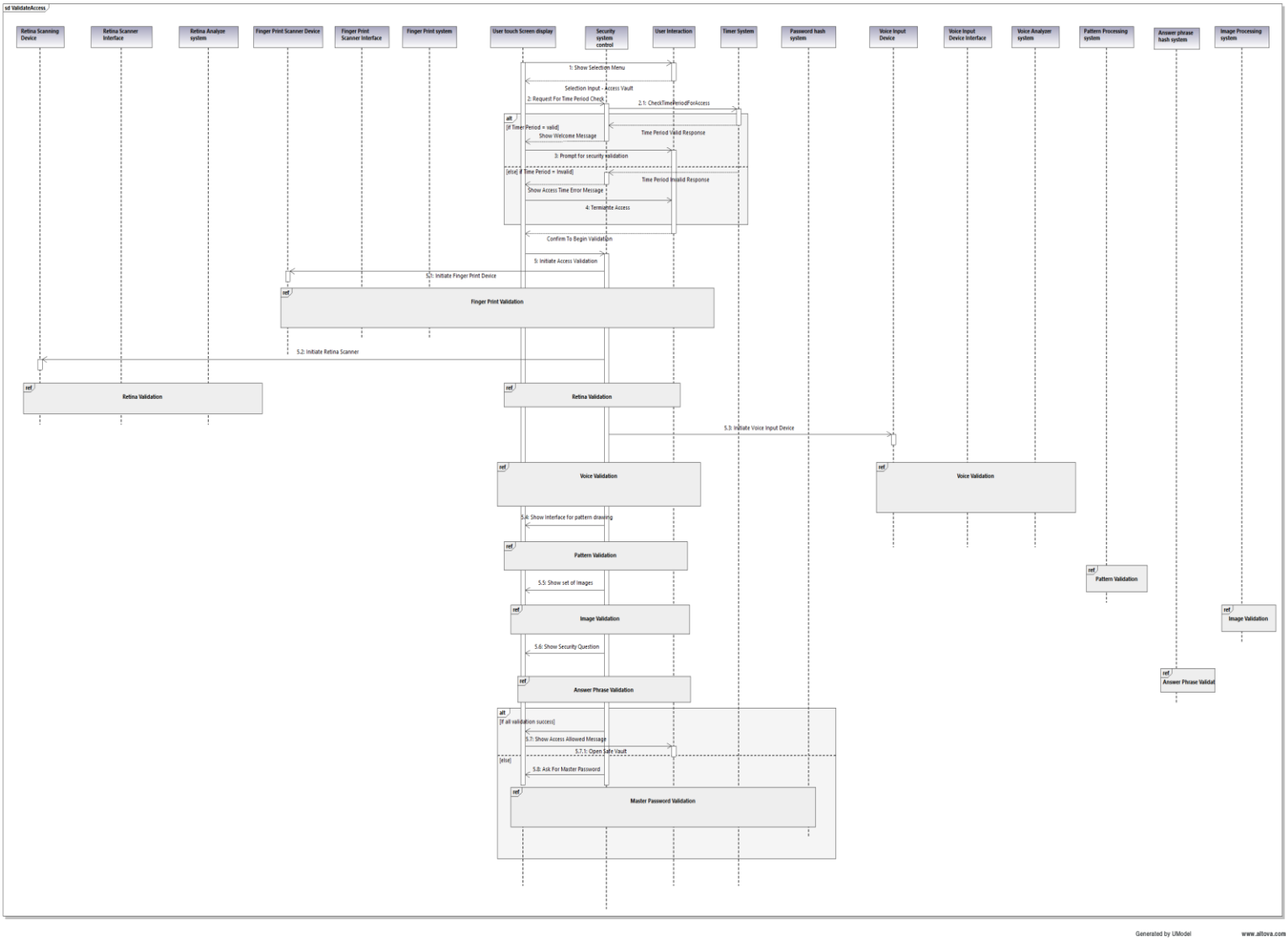
For Use Case: - Validate Security Access

Identifying the participant objects:

Since the validation request involves all the subsystem to co-operate, all the classes identified will be involved in this use case.

Sequence Diagram:

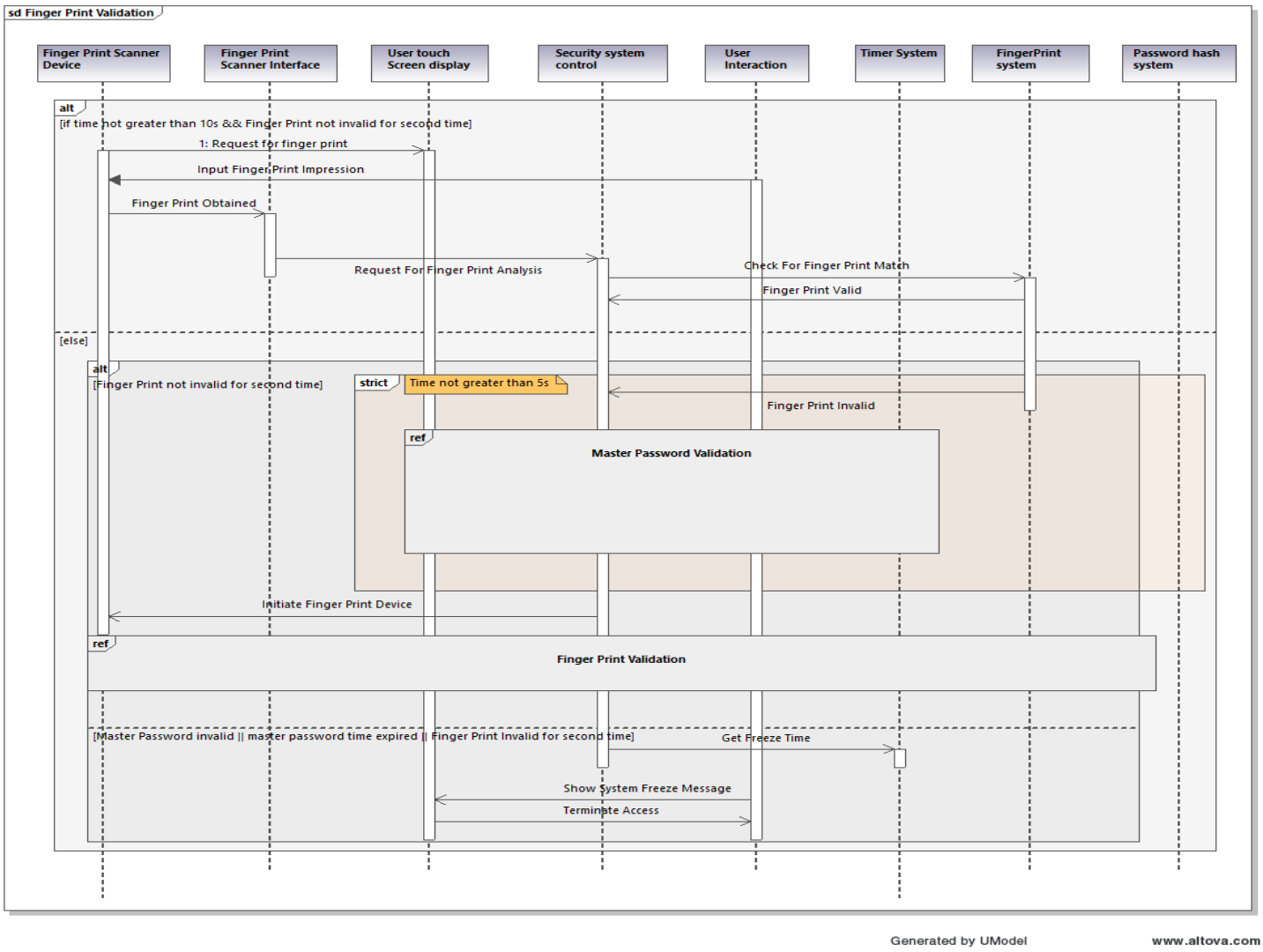
The main sequence diagram for access validation is as follows. Since the validation requires clearance of six security authentications, it is described individually and added a corresponding ref block in the main sequence diagram.



Initially system is in idle state, the user touch screen display will show the options for user. User will choose the access vault option. System checks for the time, if the time is invalid, then the user will be notified and access will be terminated. If not, then it asks for confirmation to begin the validation process. After user acknowledges, the validation process begins with finger print scanning validation. Secondly with retina pattern validation then voice validation then pattern validation and then image validation and then finally Answer phrase validation, this is the security question validation. Master password validation is used only when any validation fails are timeout occurs.

Sequence diagram for finger print validation:

The sequence diagram for finger print validation is as follows.

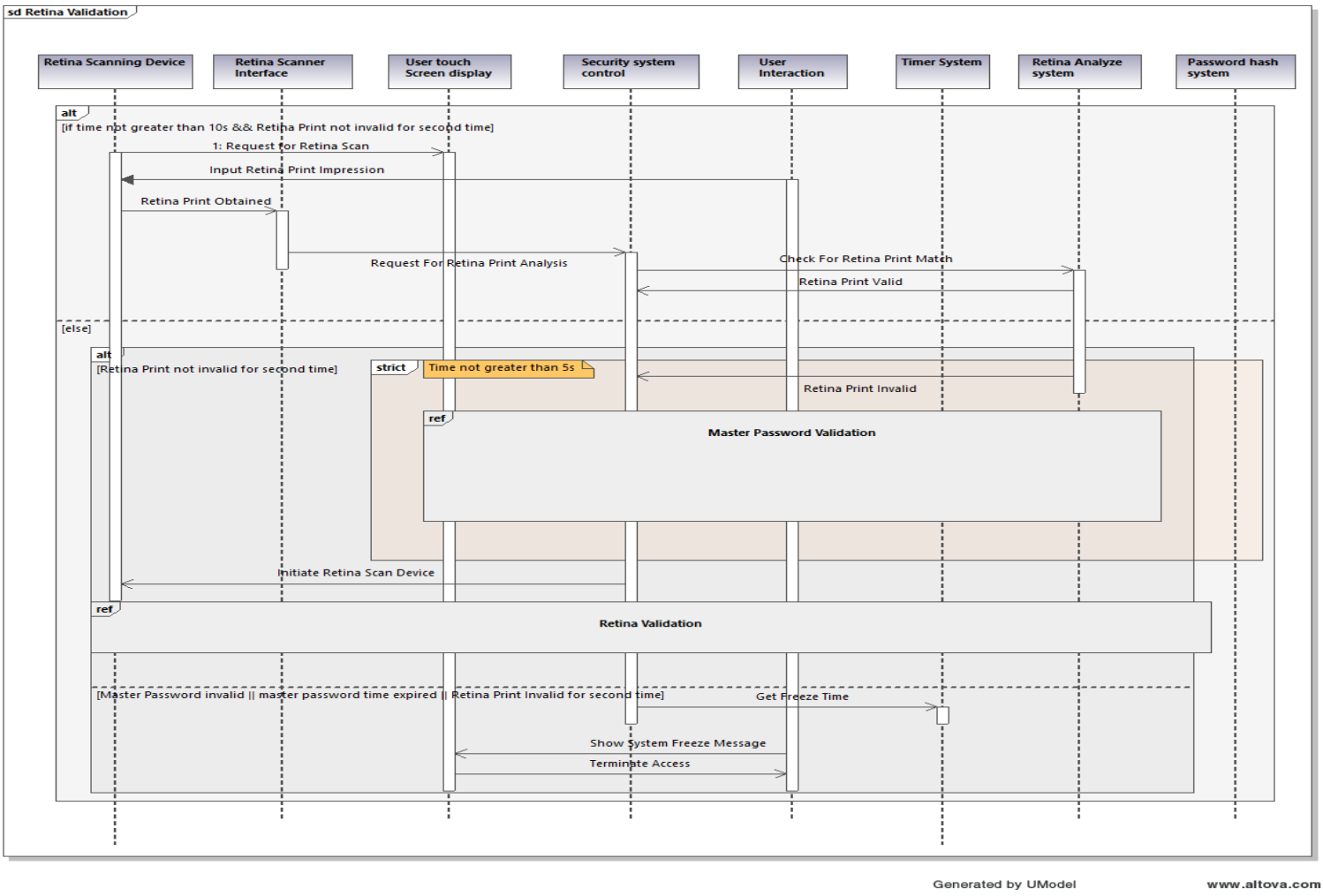


The finger print scanner will initiate the user touch screen display to display prompt for the user to input his finger print. The user gives his finger print input. The finger print is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid finger print. If the finger print is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then

the system initiates the finger print validation again. If the master password is wrong or master password time expired or finger print invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Retina Pattern validation:

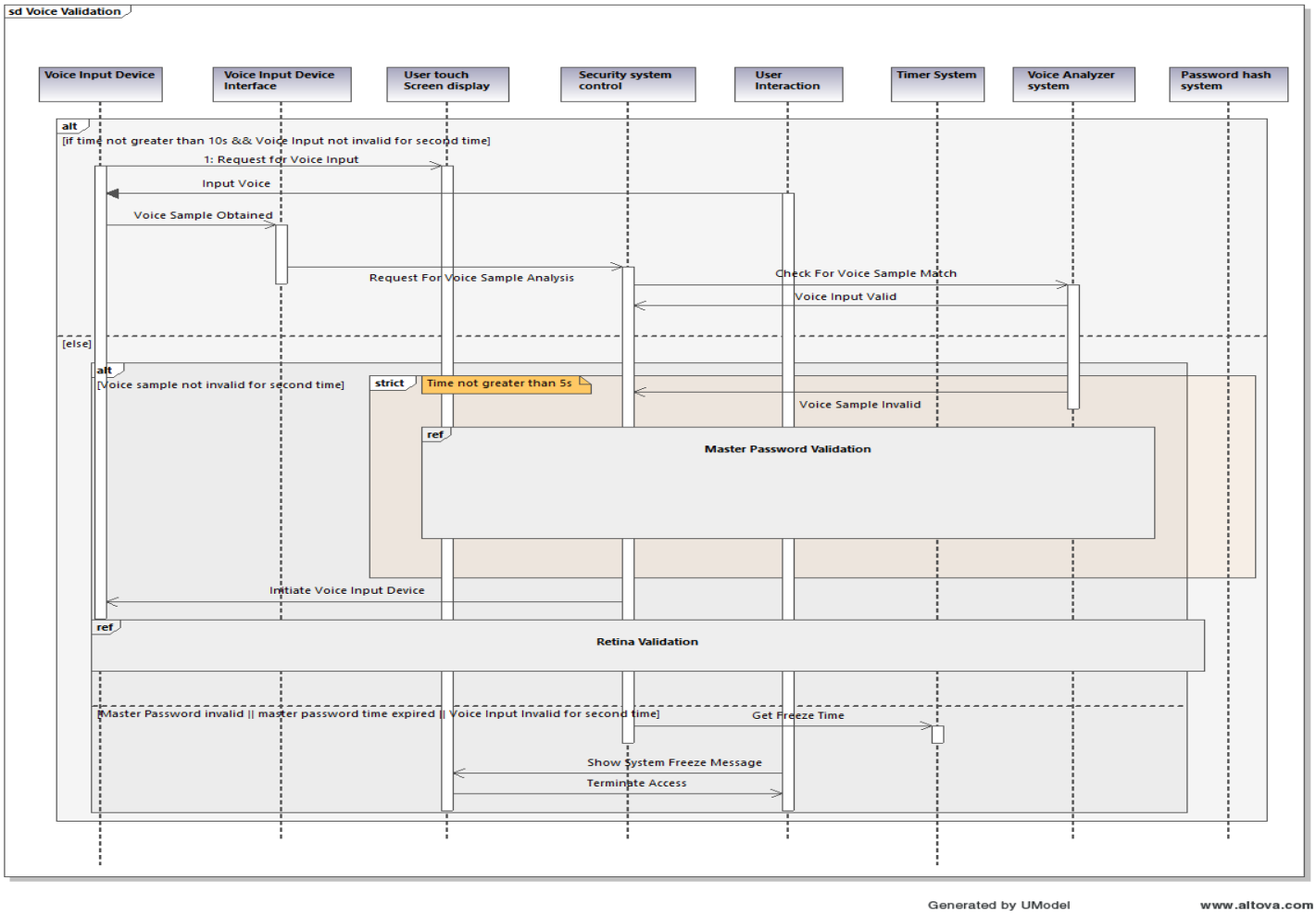
The sequence diagram for retina pattern validation is as follows.



The retina pattern scanner will initiate the user touch screen display to display prompt for the user to input his retina pattern. The user gives his retina pattern input. The retina pattern is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid retina pattern. If the retina pattern is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then the system initiates the retina pattern validation again. If the master password is wrong or master password time expired or finger print invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Voice Validation:

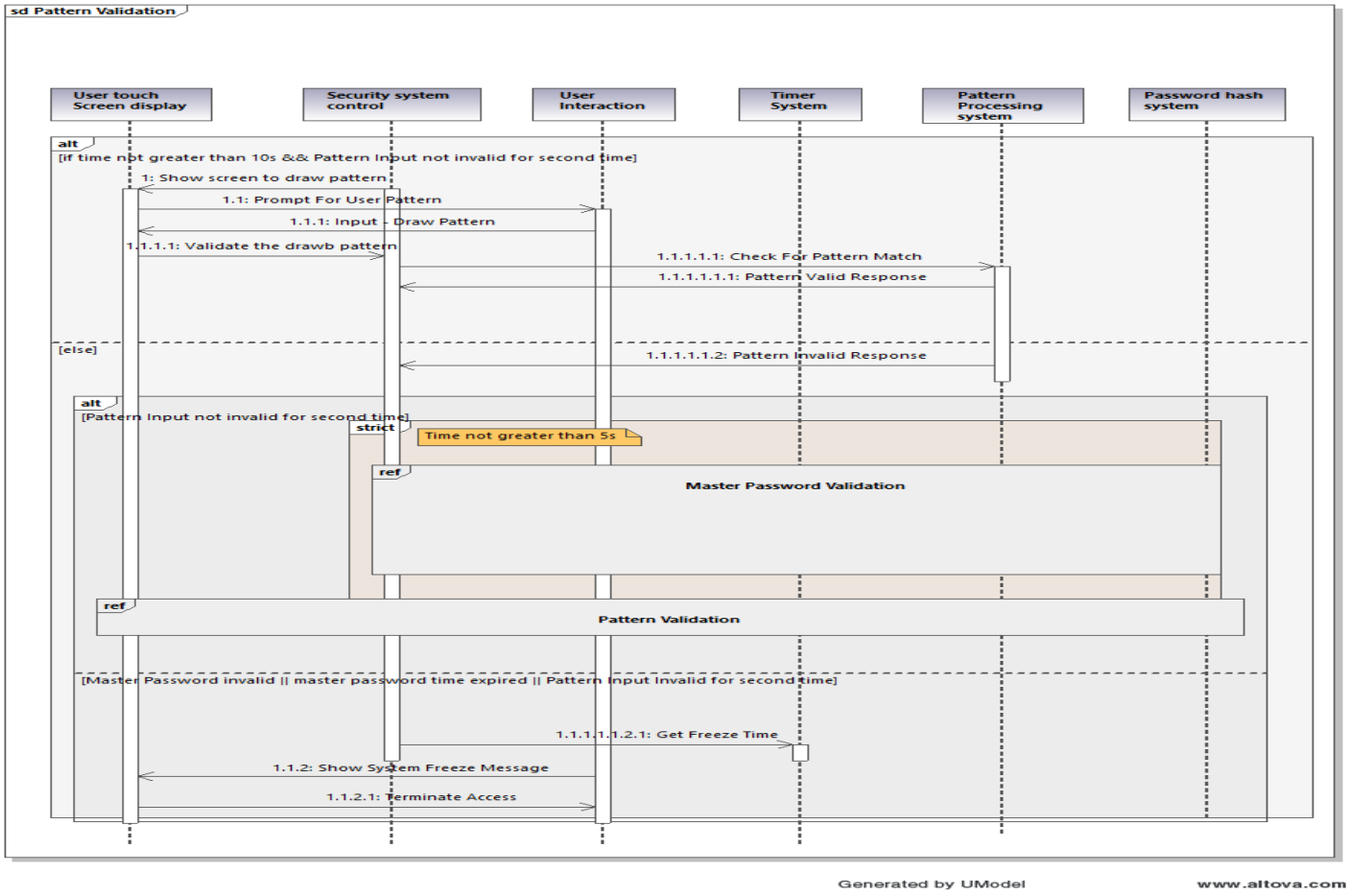
The sequence diagram for voice validation is as follows.



The voice input device will initiate the user touch screen display to display prompt for the user to input his voice. The user gives his voice input. The voice is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid voice. If the voice is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then the system initiates the voice validation again. If the master password is wrong or master password time expired or voice sample is invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Pattern Validation:

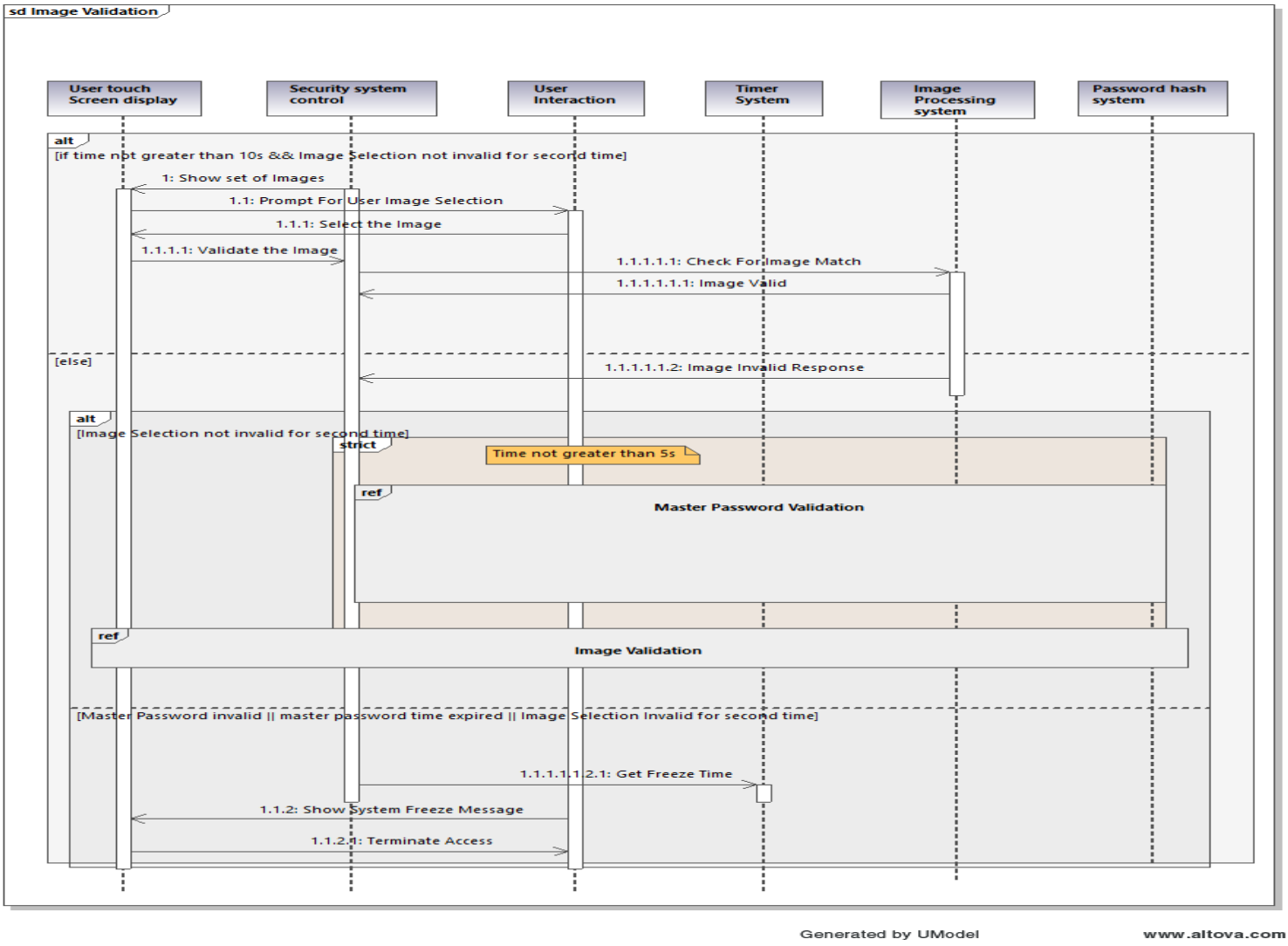
The sequence diagram for pattern validation is as follows.



The system will initiate the user touch screen display to display prompt for the user to draw his pattern. The user gives his pattern input. The pattern is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid pattern. If the pattern is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then the system initiates the pattern validation again. If the master password is wrong or master password time expired or pattern is invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Image Validation:

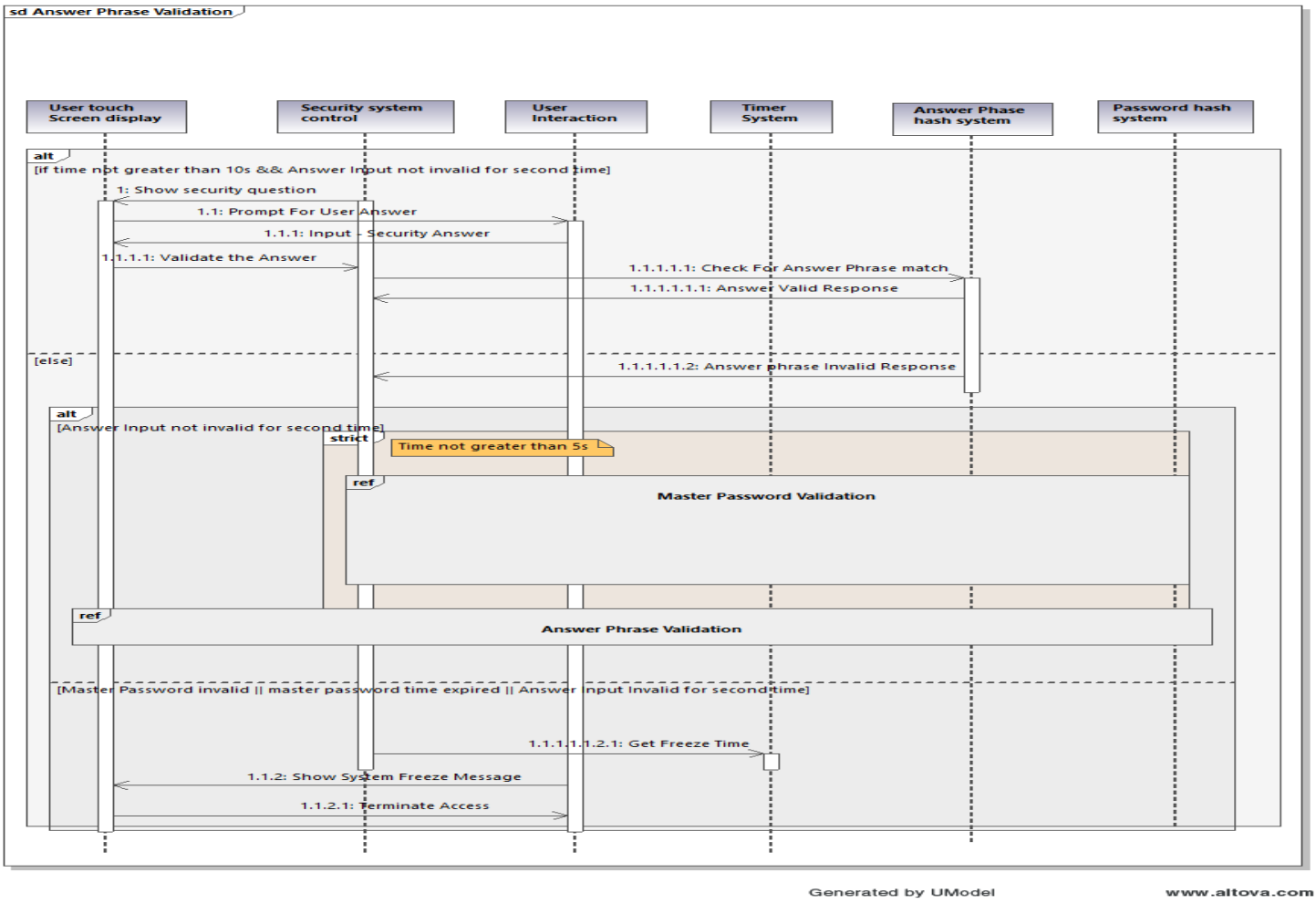
The sequence diagram for pattern validation is as follows.



The system will initiate the user touch screen display to display prompt for the user to select the image from the given set of images. The user selects his image. The image is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid pattern. If the image chosen is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then the system initiates the image validation again. If the master password is wrong or master password time expired or image selection is invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Security Question Validation:

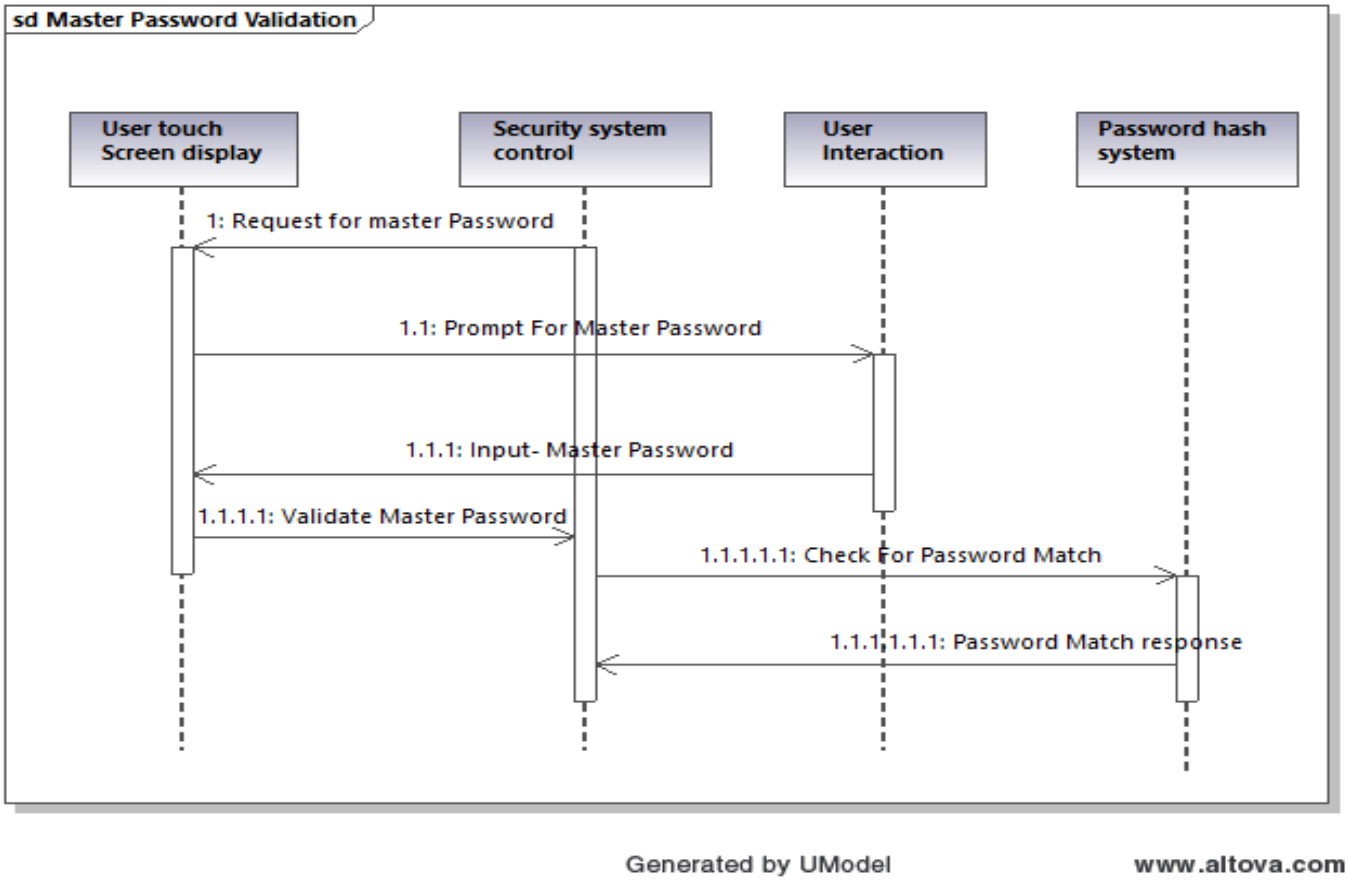
The sequence diagram for security question validation is as follows.



The system will initiate the user touch screen display to display security question for the user to input the answer. The user enters his answers. The answer is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 10s or this validation not occurring more than two times due to invalid answer. If the answer entered is invalid for first time, then the system prompts the user to enter master password within 5s. If master password is valid, then the system initiates the image validation again. If the master password is wrong or master password time expired or answer input is invalid for second time, then the system gets the freeze time from the timer and system goes into the freezing state.

Sequence Diagram for Master Password Validation:

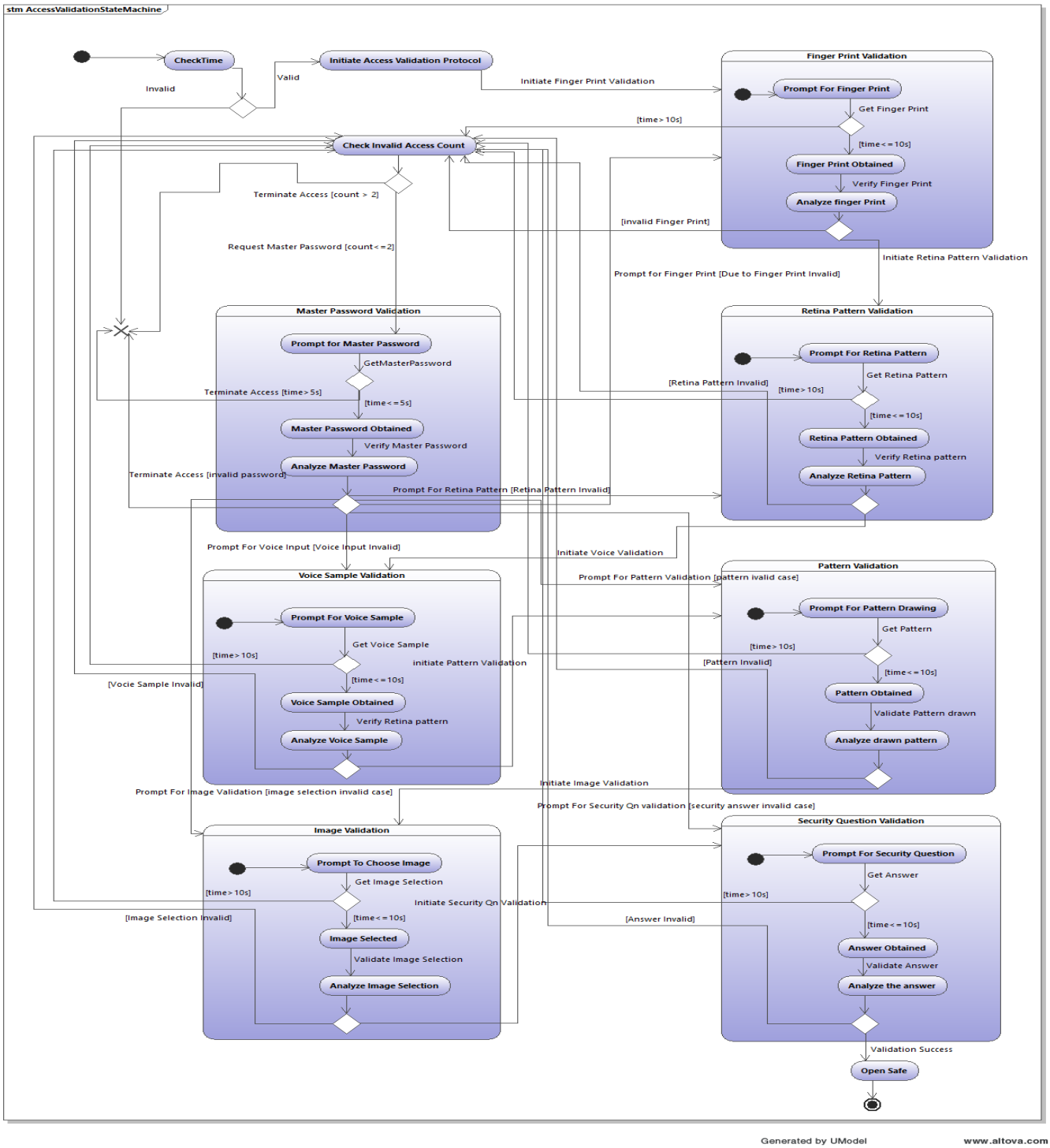
The sequence diagram for master password validation is as follows.



The system will initiate the user touch screen display to display prompt for the user to enter his master password. The user gives his master password. The password is analyzed for validity. If it is valid, then the validation is successful. This case happens only when the time period is less than or equal to 5s. If the password is invalid, then the system gets the freeze time from the timer and system goes into the freezing state.

State Machine Diagram for access validation:

The following diagram shows the state machine diagram for access validation.



Initially, security controller will be in idle state. If the access validation is invoked, it checks for time period to validate whether it is the correct time for accessing the system. If it is invalid, the state machine is terminated.

If it is valid, then it will prompt for the user to input his finger print. The user gives his finger print input. The Get Finger Print initiates a transition to a decision node where it will be analyzed that whether the finger print is obtained within 10s time frame. If it is valid, then verify finger print event causes transition to analyze the finger print obtained. If analyze finger print is successful, then the finger print validation is successful. If time period is greater than10s or finger print is invalid then it causes a transition to check invalid count state where the number of times the finger print validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated. On successfully validating the finger print, the controller initiates the retina pattern validation.

If finger print validation is successful, then it will prompt for the user to input his retina pattern. The user gives his retina pattern input. The Get Retina Pattern initiates a transition to a decision node where it will be analyzed that whether the retina pattern is obtained within 10s time frame. If it is valid, then verify retina pattern event causes transition to analyze the retina pattern obtained. If analyze retina pattern is successful, then the retina pattern validation is successful. If time period is greater than10s or retina pattern is invalid then it causes a transition to check invalid count state where the number of times the retina pattern validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated. On successfully validating the retina pattern, the controller initiates the voice validation.

If retina pattern validation is successful, then it will display prompt for the user to input his voice. The user gives his voice input. The GetVoiceSample initiates a transition to a decision node where it will be analyzed that whether the voice sample is obtained within 10s time frame. If it is valid, then verify voice sample event causes transition to analyze the voice sample obtained. If analyze voice sample is successful, then the voice sample validation is successful. If time period is greater than10s or voice sample is invalid then it causes a transition to check invalid count state where the number of times the voice sample validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated. On successfully validating the voice sample, the controller initiates the pattern validation.

If the voice validation is successful, then it will prompt for the user to draw his pattern. The user gives his pattern input. The Get pattern initiates a transition to a decision node where it will be analyzed that whether the pattern is obtained within 10s time frame. If it is valid, then validate pattern drawn event causes transition to analyze the pattern obtained. If analyze pattern is successful, then the pattern validation is successful. If time period is greater than10s or pattern drawn is invalid then it causes a transition to check invalid count state where the number of times the pattern validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated. On successfully validating the pattern drawn, the controller initiates the image validation.

If the pattern validation is successful, then it will prompt for the user to select the image from the given set of images. The user selects his image. The Get Image initiates a transition to a decision node where it will be analyzed that whether the pattern is obtained within 10s time frame. If it is valid, then validate pattern drawn event causes transition to analyze the pattern obtained. If analyze pattern is successful, then the pattern validation is successful. If time period is greater than10s or pattern drawn is invalid then it causes a transition to check invalid count state where the number of times the pattern validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated. On successfully validating the image, the controller initiates the security question answer validation.

If the image validation is successful, then it will display security question for the user to input the answer. The user enters his answers. The Get Answer initiates a transition to a decision node where it will be analyzed that whether the answer entered is obtained within 10s time frame. If it is valid, then validate answer event causes transition to analyze the answer obtained. If analyze the answer is successful, then the answer validation is successful. If time period is greater than10s or answer entered is invalid then it causes a transition to check invalid count state where the number of times the answer validation is failed is checked. If it is greater than two, then it will go to terminate state where access is terminated. If the count is less than or equal to 2, then the master password validation state is invoked where it will prompt for master password. The user gives the master password. If the master password is entered within 5s, then validate master password state is invoked where the master password is validated. If the master password is wrong or the master password has not been got within 5s then it will go to terminate access state where the user access is terminated.

Thus by validating all security access methods, the transition is made to open safe which represents the safe vault being opened successfully. Finally the state machine reaches its final state.

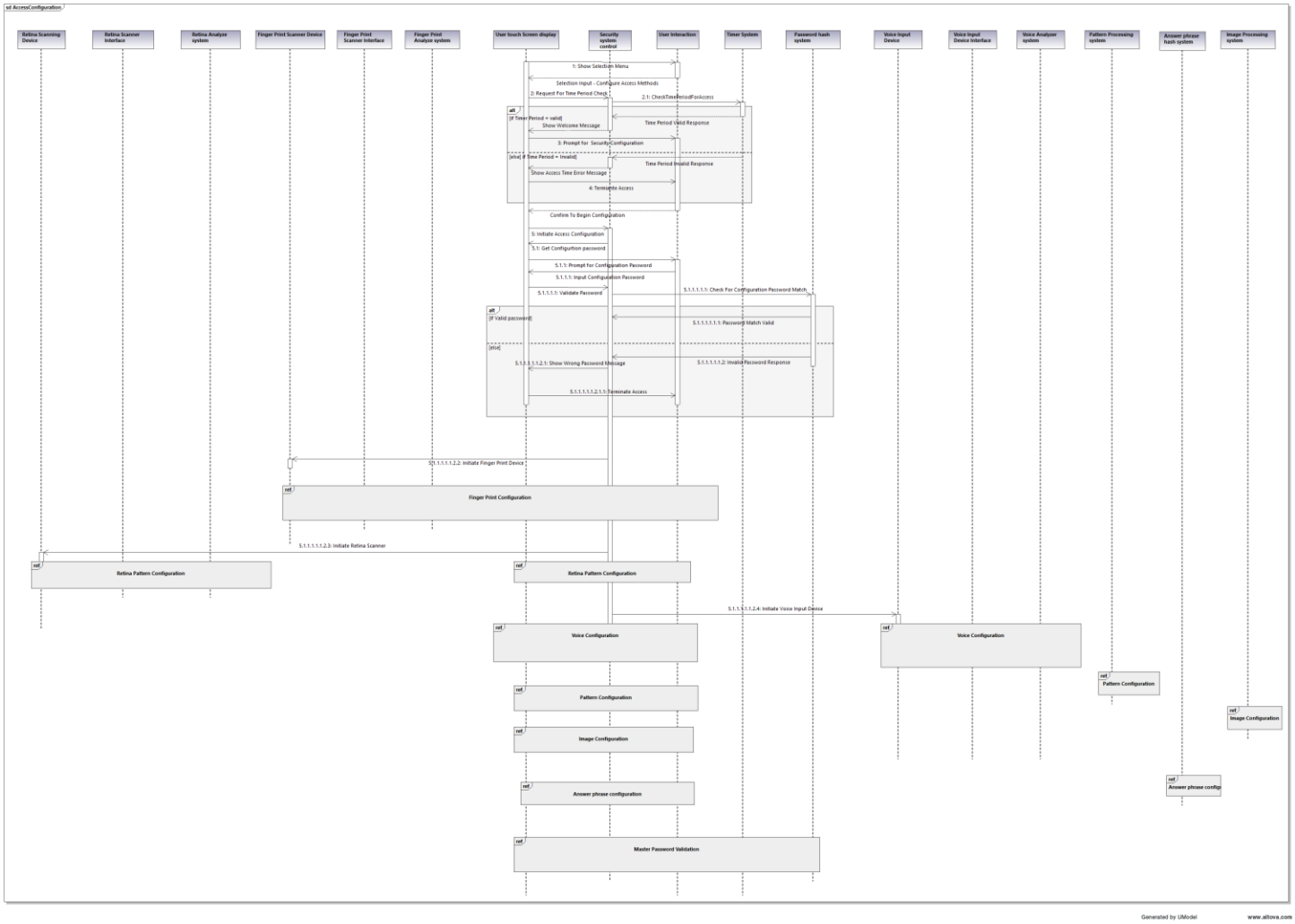
For Use Case: - Configure Security Access

Identifying the participant objects:

Since the configuration request involves all the subsystem to co-operate, all the classes identified will be involved in this use case.

Sequence Diagram:

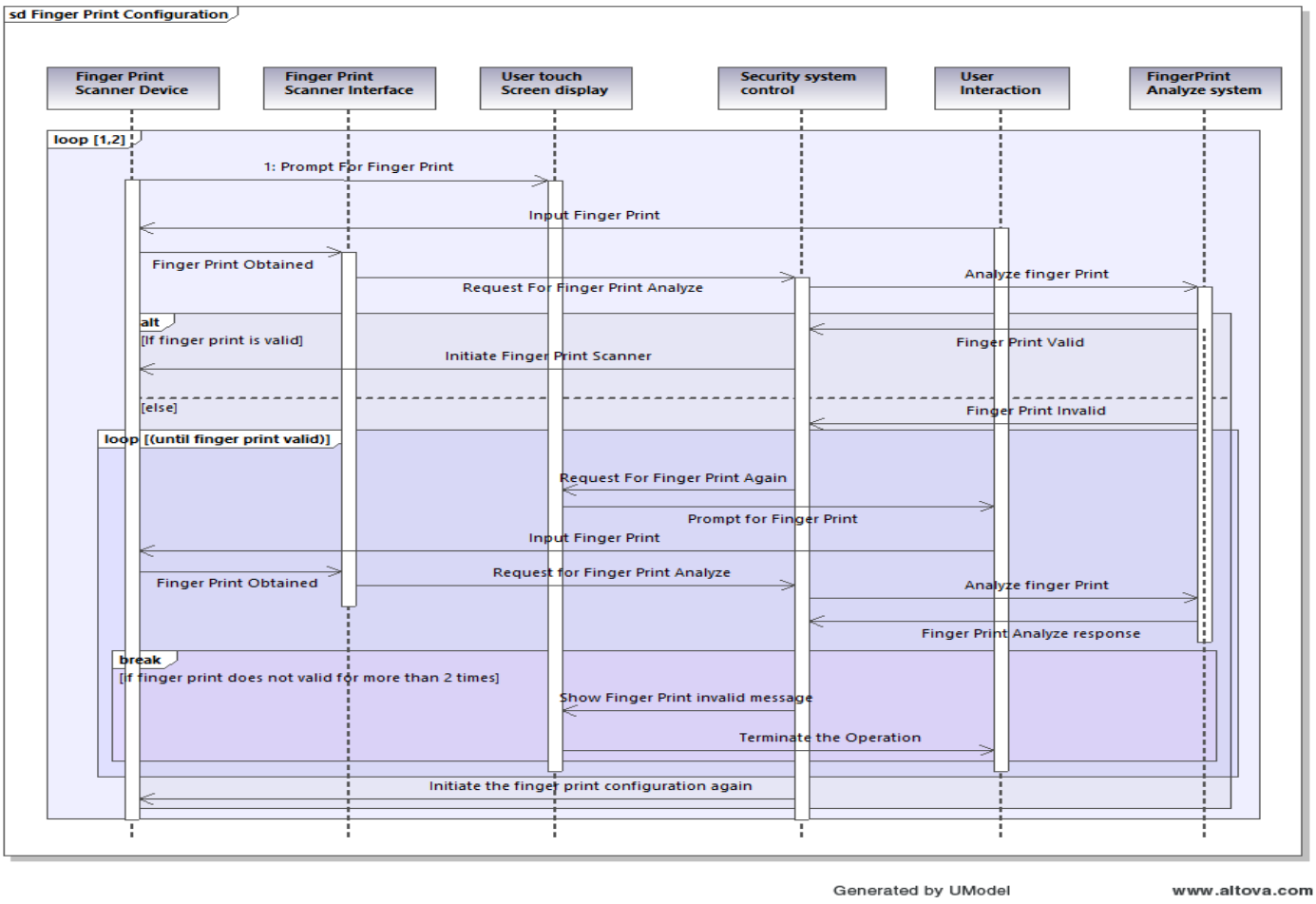
The main sequence diagram for access configuration is as follows. Since the configuration requires defining six security authentications, it is described individually and added a corresponding ref block in the main sequence diagram.



Initially system is in idle state, the user touch screen display will show the options for user. User will choose the configure access option. System checks for the time, if the time is invalid, then the user will be notified and access will be terminated. If not, then it asks for confirmation to begin the validation process. After user acknowledges, the validation process begins by getting the configuration password. If the configuration password is invalid, then the access is terminated else it will begin with finger print configuration. Secondly with retina pattern configuration then voice configuration then pattern configuration and then image configuration and then Answer phrase configuration, this is the security question configuration and finally Master password configuration done.

Sequence diagram for finger print configuration:

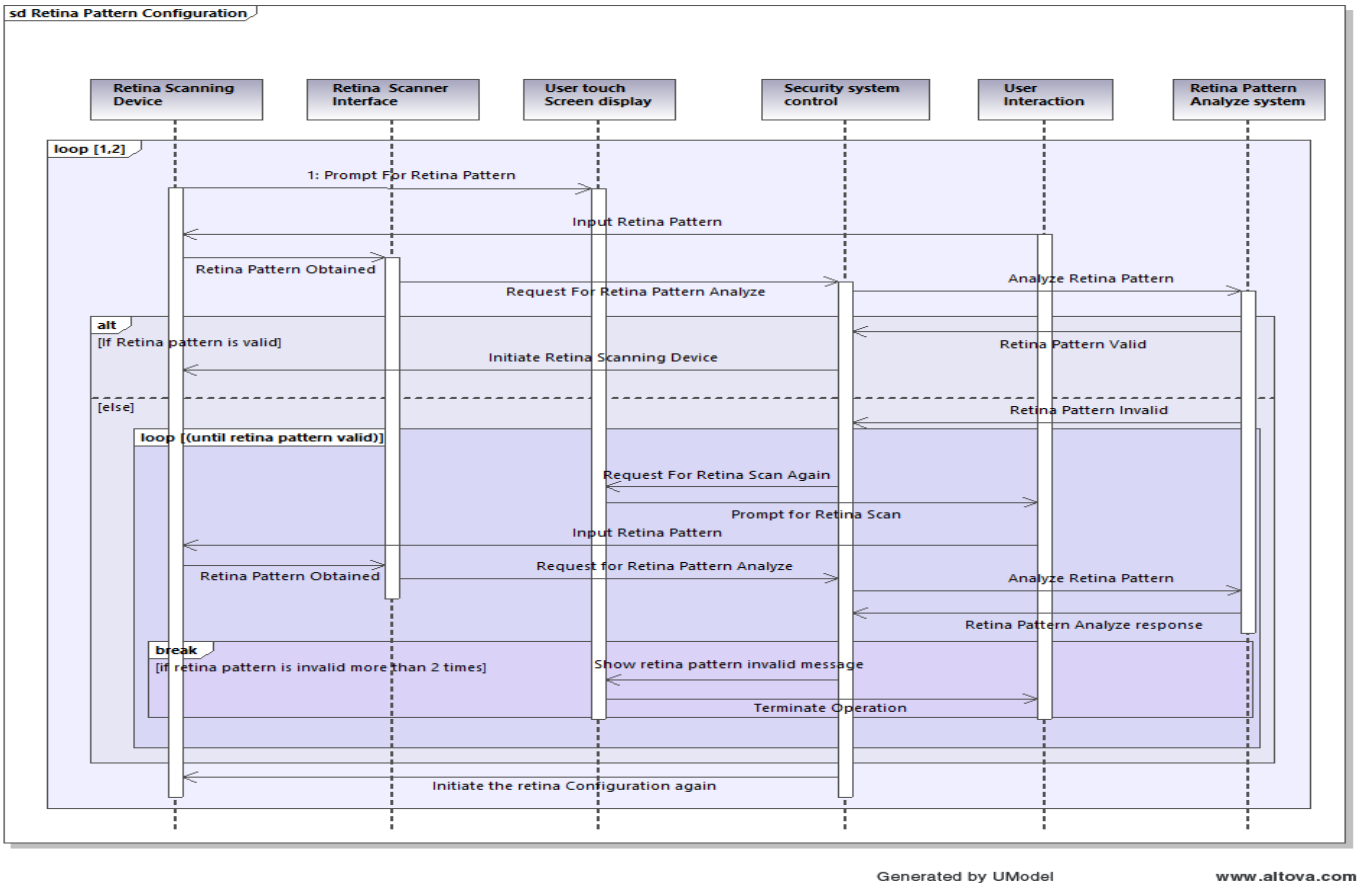
The sequence diagram for finger print configuration is as follows.



The finger print scanner will initiate the user touch screen display to display prompt for the user to input his finger print. The user gives his finger print input. The finger print is analyzed for validity. If it is valid, then the system asks for second finger print and it is also analyzed. If that is also successful, then the configuration of finger print is successful. If any one of the finger print is not valid, then the system will loop to get the finger print until it gets a valid print. But if the user keeps on giving the wrong finger print, then the loop will break and current operation is terminated and the system reinitiates the finger print configuration again.

Sequence diagram for retina pattern configuration:

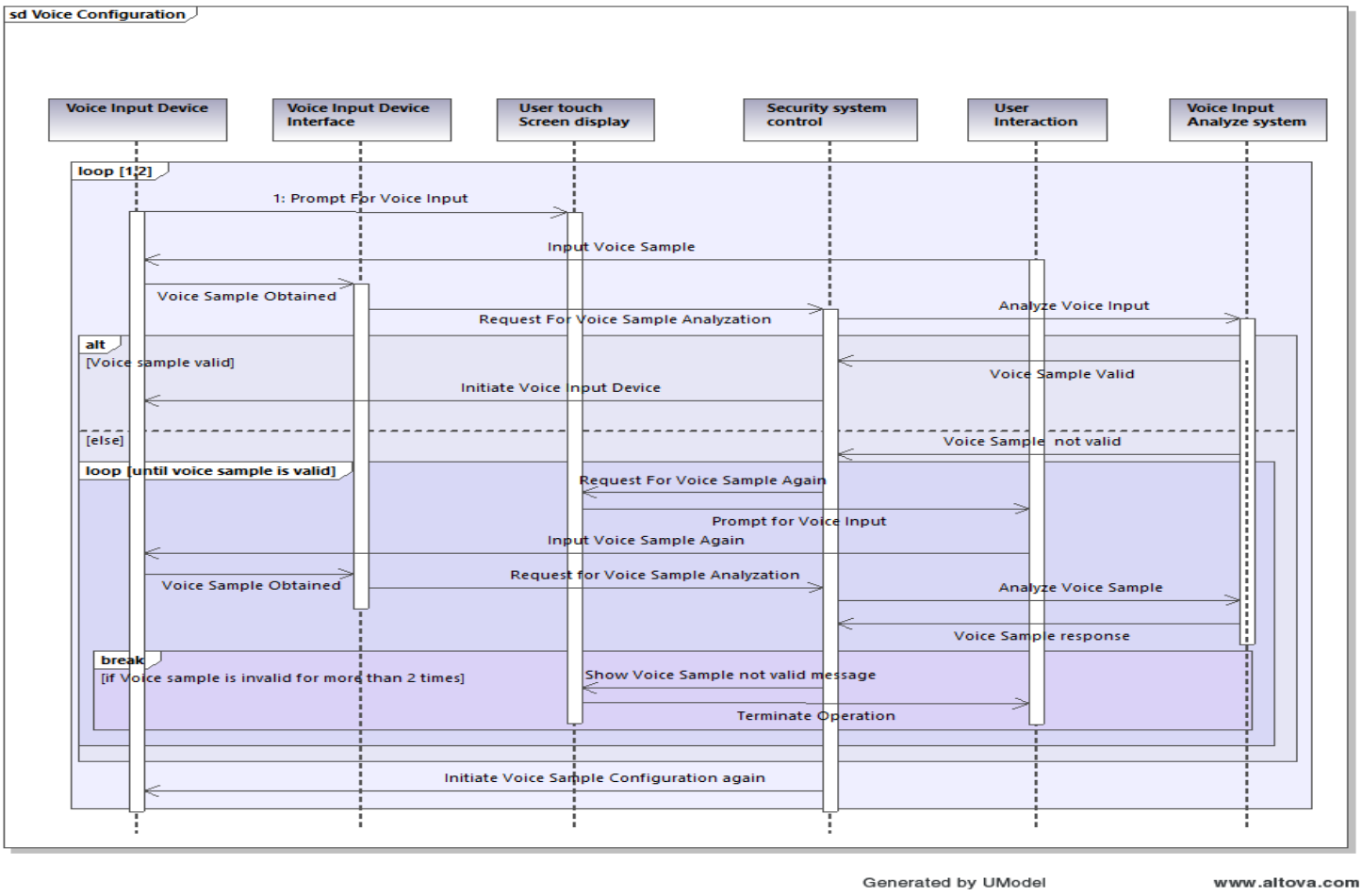
The sequence diagram for retina pattern configuration is as follows.



The retina pattern scanner will initiate the user touch screen display to display prompt for the user to input his retina pattern. The user gives his retina pattern. The retina pattern is analyzed for validity. If it is valid, then the system asks for second retina print and it is also analyzed. If that is also successful, then the configuration of retina pattern is successful. If any one of the retina pattern is not valid, then the system will loop to get the retina pattern until it gets a valid retina pattern. But if the user keeps on giving the wrong retina pattern, then the loop will break and current operation is terminated and the system reinitiates the retina pattern configuration again.

Sequence diagram for voice configuration:

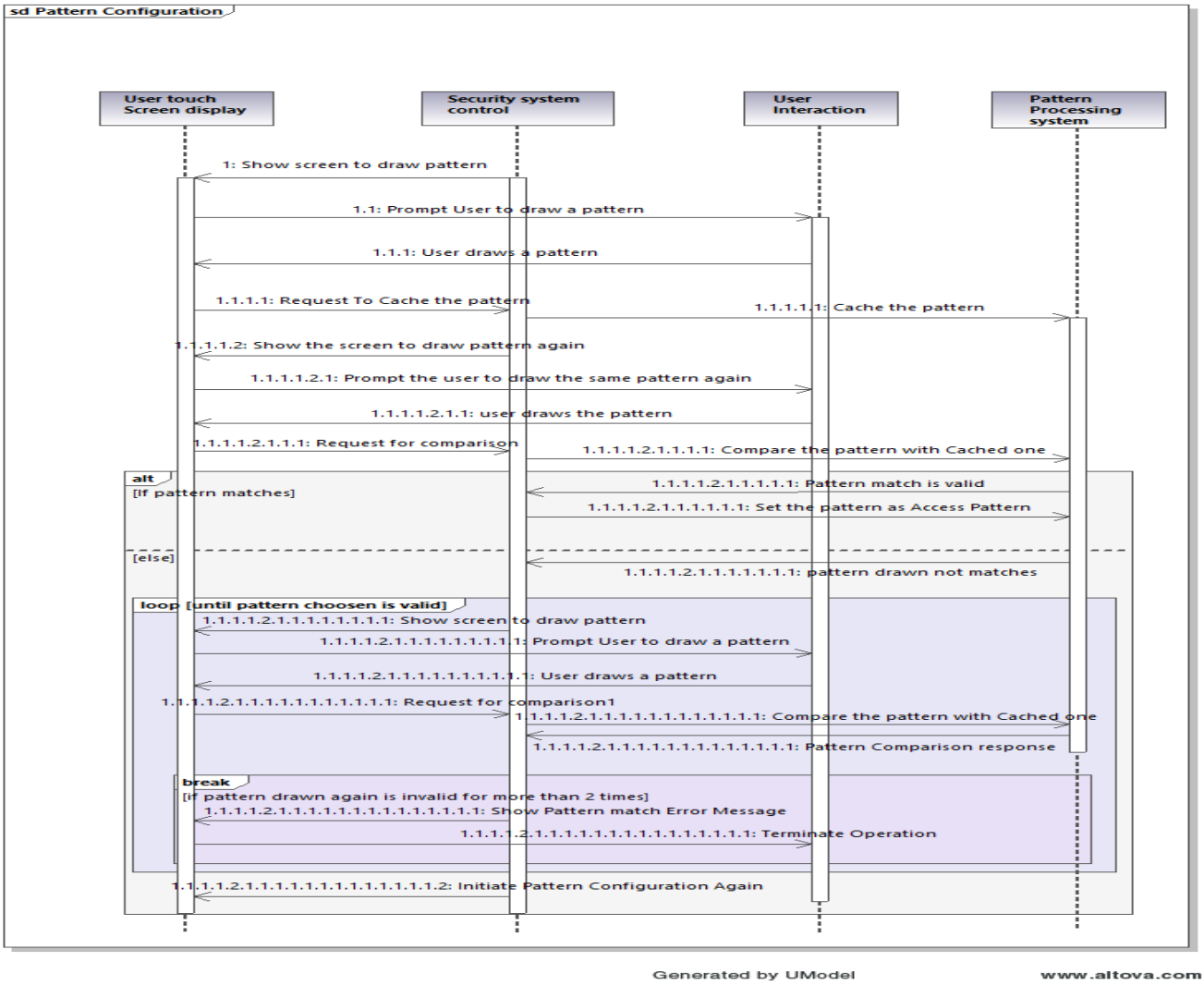
The sequence diagram for voice configuration is as follows.



The voice input device will initiate the user touch screen display to display prompt for the user to input his voice. The user gives his voice sample. The voice sample is analyzed for validity. If it is valid, then the system asks for voice sample for second time and it is also analyzed. If that is also successful, then the configuration of voice sample is successful. If any one of the voice sample is not valid, then the system will loop to get the voice sample until it gets a valid voice sample. But if the user keeps on giving the wrong voice sample, then the loop will break and current operation is terminated and the system reinitiates the voice sample configuration again.

Sequence diagram for pattern configuration:

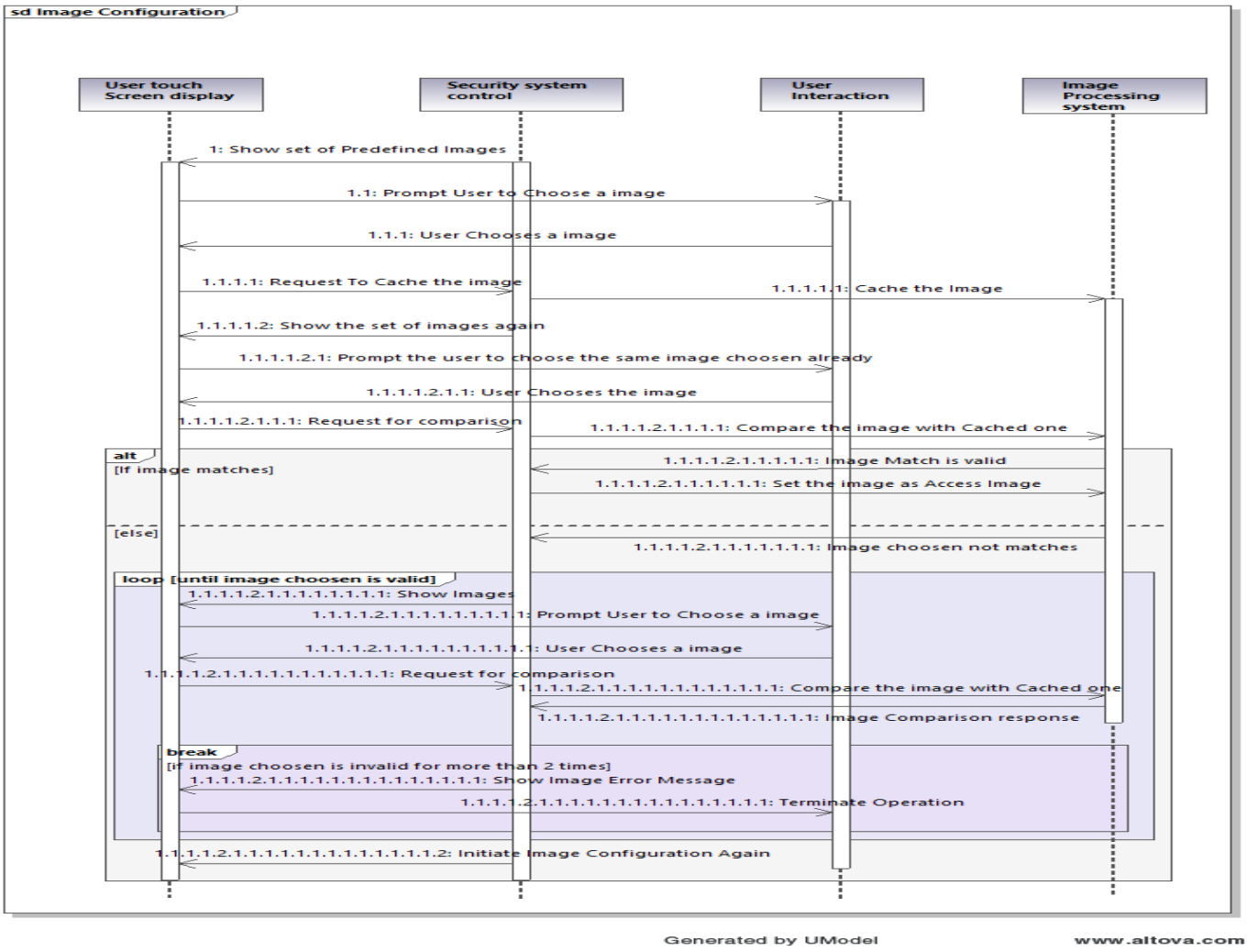
The sequence diagram for pattern configuration is as follows.



The security control will initiate the user touch screen display to display prompt for the user to draw his pattern. The user draws his pattern. The pattern is cached. Then the system asks for pattern for second time and it is also analyzed and sees for match. If that is successful, then the configuration of pattern is successful. If the second drawn pattern is not valid, then the system will loop to get the pattern until it gets a valid pattern. But if the user keeps on giving the wrong pattern, then the loop will break and current operation is terminated and the system reinitiates the pattern configuration again.

Sequence diagram for image configuration:

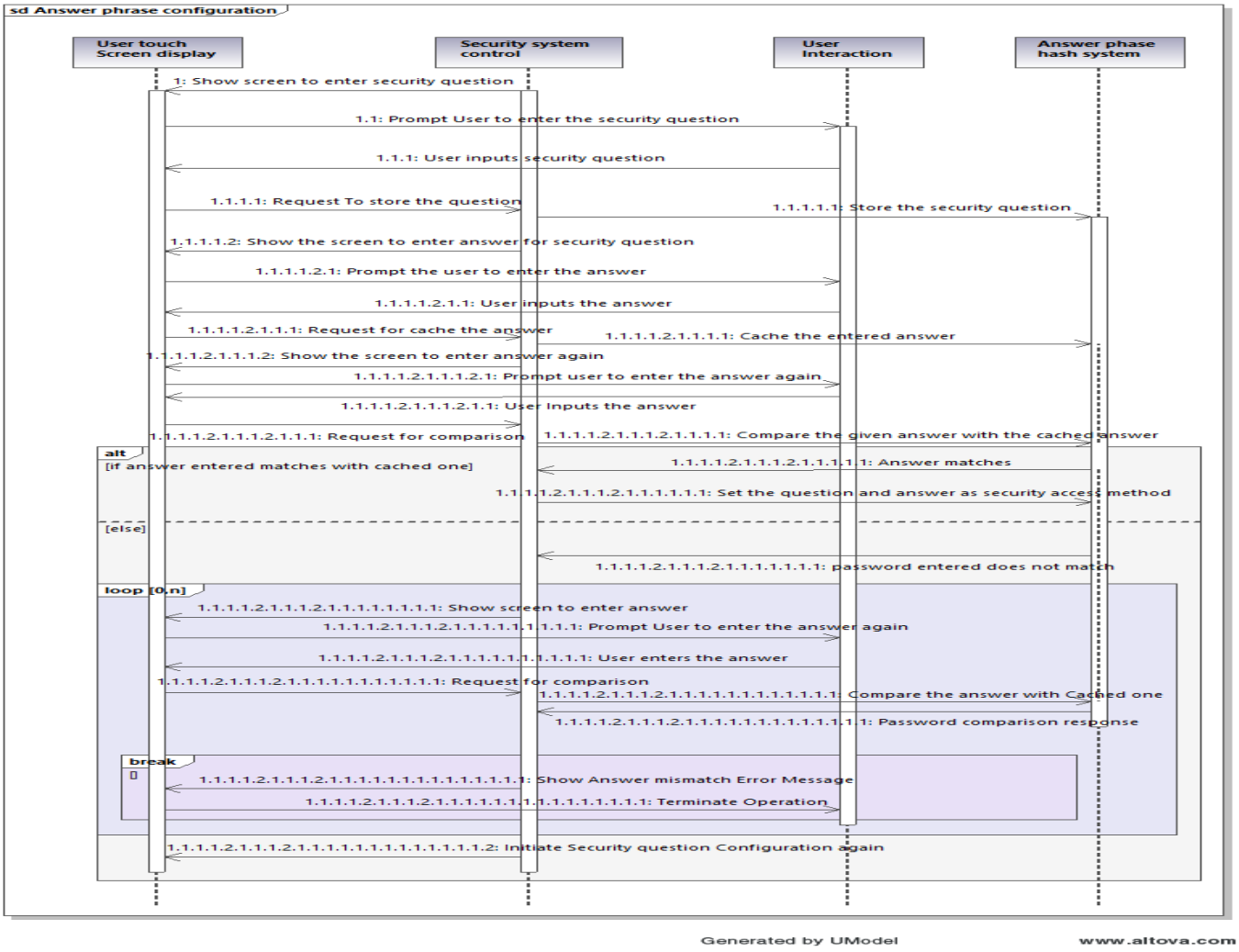
The sequence diagram for image configuration is as follows.



The security control will initiate the user touch screen display to display prompt for the user to choose his image. The user selects the image. The image is cached. Then the system asks for image for second time and it is compared with previous selected image and sees for match. If that is successful, then the configuration of image is successful. If the second image is not valid, then the system will loop to get the right image selected until it gets a correct image. But if the user keeps on selecting the wrong image, then the loop will break and current operation is terminated and the system reinitiates the image configuration again.

Sequence diagram for security question configuration:

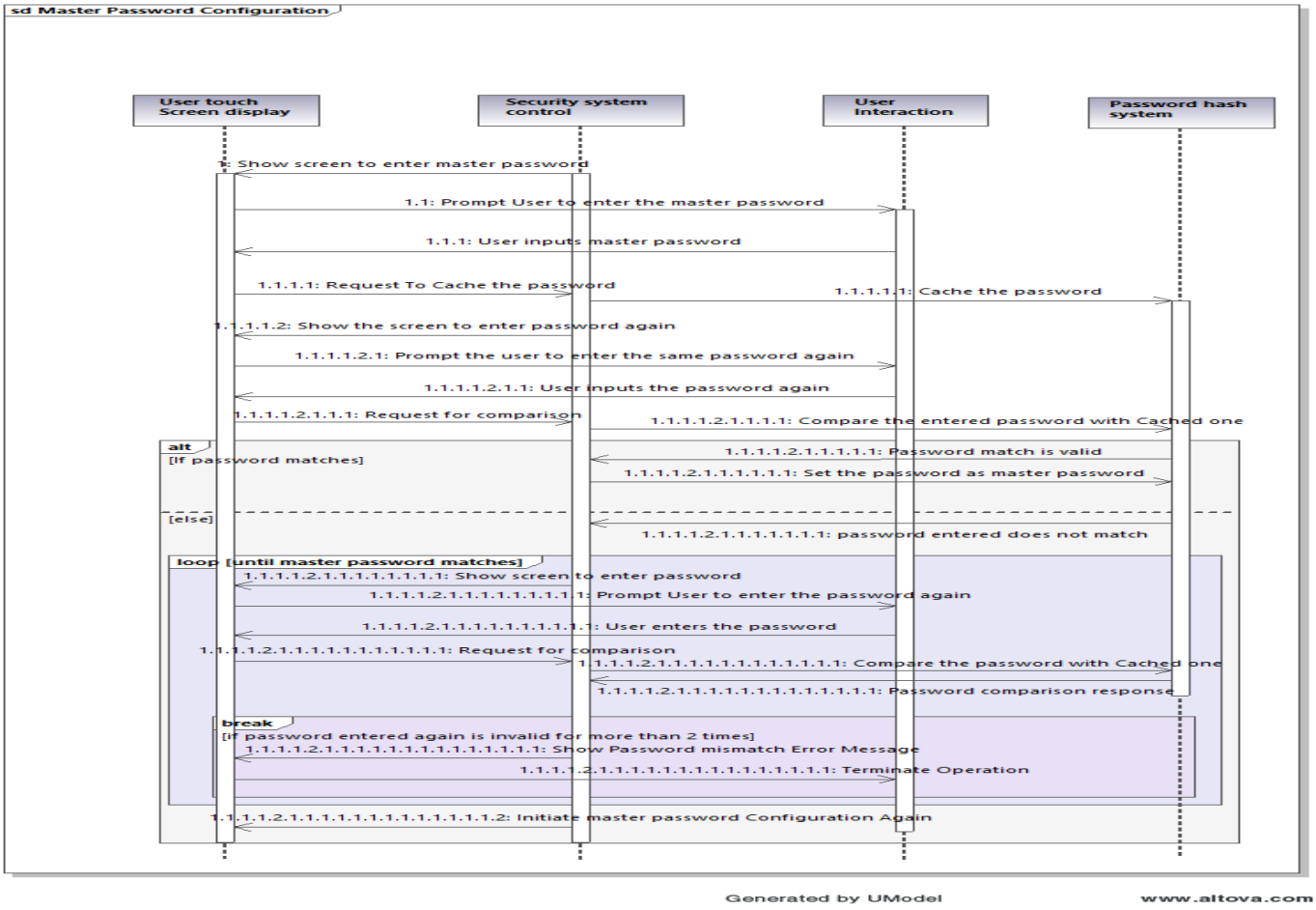
The sequence diagram for security question configuration is as follows.



The security control will initiate the user touch screen display to display prompt for the user to enter the security question. The user enters the security question. The security question is stored. Then the system prompts for answer to the security question. The user enters the security answer. The answer is cached. Again the system prompts user to enter the answer again to double check. The user enters the answer. The system analyze for match. If it matches, then the configuration of security question is successful. If no match, then the system loops to get the right answer, if the user keeps on giving wrong input then the loop breaks and reinitiates the security question configuration again.

Sequence diagram for master password configuration:

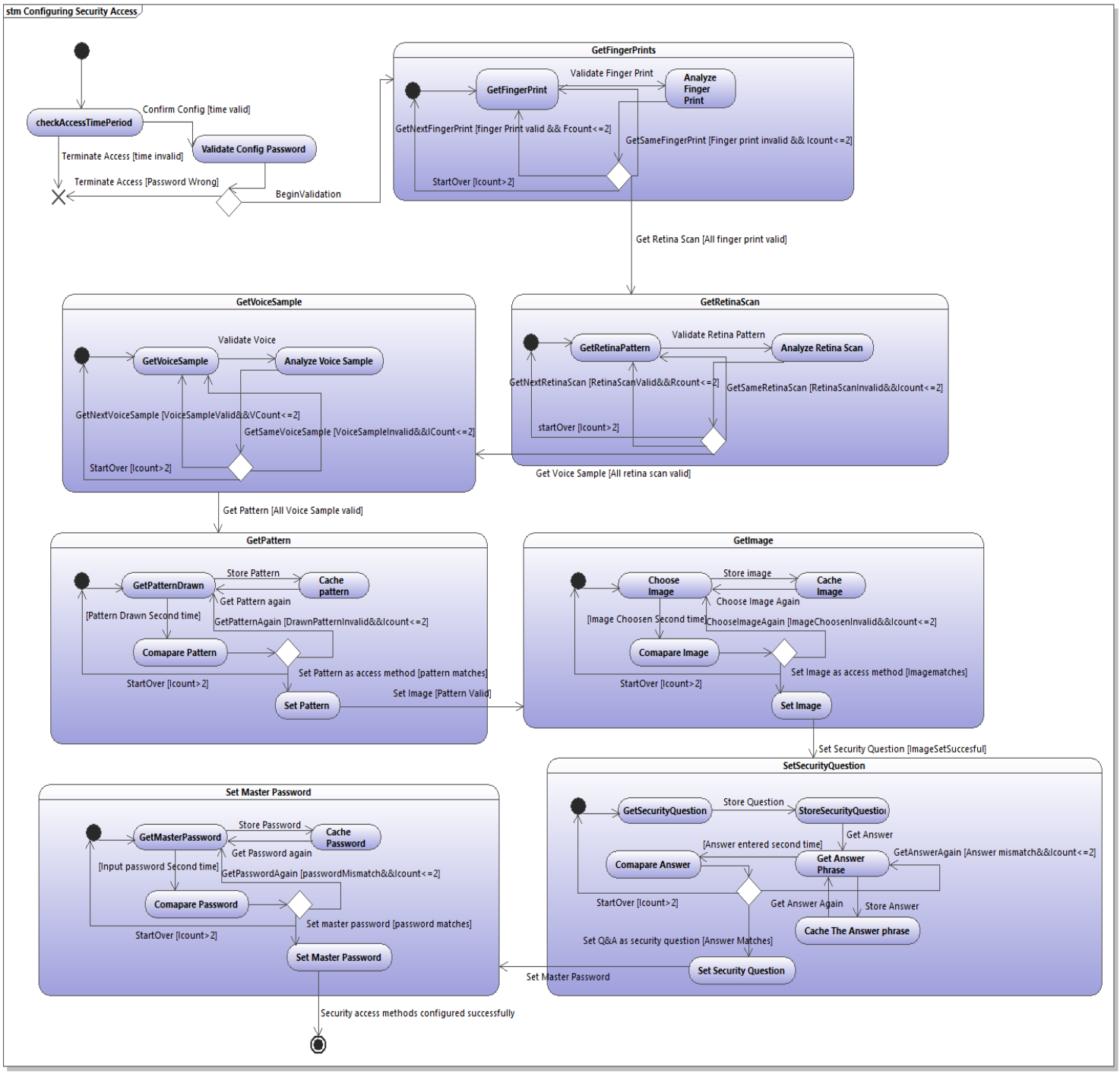
The sequence diagram for master password configuration is as follows.



The security control will initiate the user touch screen display to display prompt for the user to enter his master password. The user inputs his master password. The password is cached. Then the system asks for password for second time and it is analyzed and sees for match. If that is successful, then the configuration of master password is successful. If the second drawn password is not valid, then the system will loop to get the password until it gets a valid password. But if the user keeps on giving the wrong password, then the loop will break and current operation is terminated and the system reinitiates the master password configuration again.

State Machine Diagram for configuring security access:

The following diagram shows the state machine diagram for configuring security access.



.

Initially the controller will be in idle state, when the user chooses to configure the access methods, it will check for time period validity for access. If it is valid, then the configuration password entered is checked. If the configuration password is not valid, then the access is terminated.

If the configuration password is valid, then the beginvalidation event initiates the transition to getfingerprints composite state where the finger print is obtained in GetFingerPrint state and validate finger print event causes the transition to analyze finger print state where the finger print is analyzed for validity. If the finger print is valid, then the second finger print is obtained. If not, then state loops until it gets a valid print. The breaking point is invalid count of more than 2 where it initiates the finger print again. If the finger prints are valid, then the finger print is set for finger print validation.

After successfully getting finger prints, get retina pattern initiates the transition to GetRetinaPattern state. In this state, the retina pattern is obtained in GetRetinaPattern state and validate retina pattern event causes the transition to analyze retina pattern state where the retina pattern is analyzed for validity. If the retina pattern is valid, then the second retina pattern is obtained. If not, then state loops until it gets a valid retina pattern. The breaking point is invalid count of more than 2 where it initiates the retina pattern configuration again. If the retina patterns are valid, then the pattern is set for retina pattern validation.

After successfully getting retina patterns, get voice sample initiates the transition to GetVoiceSample state. In this state, the voice sample is obtained in GetVoiceSample state and validate voice sample event causes the transition to analyze voice sample state where the voice sample is analyzed for validity. If the voice sample is valid, then one more time voice sample is obtained for reliability. If not, then state loops until it gets a valid voice sample. The breaking point is invalid count of more than 2 where it initiates the voice sample configuration again. If the voice samples are valid, then the voice is set for voice validation.

After successfully getting voice samples, get pattern initiates the transition to GetPattern state. In this state, the pattern drawn is obtained in GetPatternDrawn state and store pattern transition caches the pattern temporarily. Then get pattern again initiates the transition to GetPatternDrawn state again where the pattern is obtained again. Then the pattern drawn second time initiates the transition to compare pattern state where the pattern drawn is compared for validity. If the pattern drawn is not valid, then state loops until it get a correct pattern what the user has drawn first. The breaking point is invalid count of more than 2 where it initiates the pattern configuration again. If the patterns drawn are valid, then the pattern is set for pattern validation in set pattern state.

After successfully getting pattern, set image initiates the transition to GetImage state. In this state, the image selected is obtained in chooseImage state and store image transition caches the images temporarily. Then choose image again initiates the transition to chooseImage state again where the image is selected again. Then the image selected second time initiates the transition to compare image state where the image selected is compared for validity. If the image selected is not valid, then state loops until it get a correct pattern what the user has drawn first. The breaking point is invalid count of more than 2 where it initiates the image configuration again. If the image selections are valid, then the image is set for image validation in set image state.

After successfully getting image, set security question initiates the transition to SetSecurityQuestion state. In this state, the security question is obtained in getsecurityquestion state and store security question transition stores the security question. Then get answer state initiates the transition to get answer phrase state where the answer for the security question is entered. Then the get answer again initiates the transition again to get answer state where the answer is entered again. Then the answer selected second time initiates the transition to compare answer state where the answer entered is compared for validity. If the answer entered is not valid, then state loops until it get a correct answer what the user has entered first. The breaking point is invalid count of more than 2 where it initiates the security question configuration again. If the security question and answers are valid, then it is set for security question validation in set security question state.

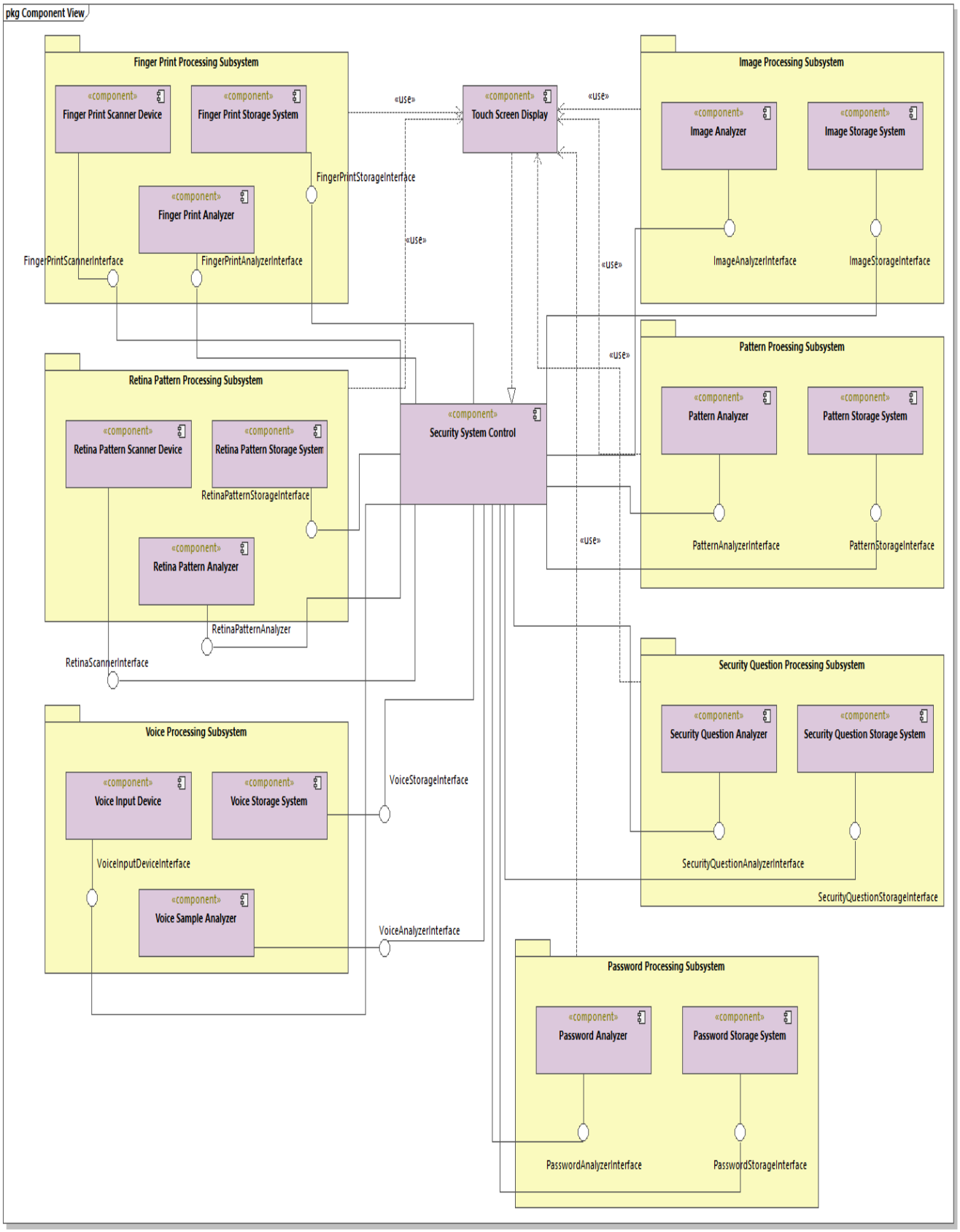
After successfully getting security question, set master password initiates the transition to Set Master Password state. In this state, the password entered is obtained in GetMasterPassword state and store password transition caches the password temporarily. Then get password again initiates the transition to GetMasterPassword state again where the password is selected again. Then the password entered second time initiates the transition to compare password where the password entered is compared for validity. If the password entered is not valid, then state loops until it get a correct password what the user has entered first. The breaking point is invalid count of more than 2 where it initiates the master password configuration again. If the master password entered is valid, then it is set as master password for master password validation.

When all the security access methods are configured successfully, the state machine reaches the final state and it is ready for validation for access.

Design Model

Structuring the application to Sub-system and defining the interface:

The following diagram shows the various sub-system and interface between them and the security control.



From this diagram, we can see that there are seven sub-systems namely finger print processing, retina pattern processing, image processing, voice processing, pattern processing, security question processing, password processing.

Finger print subsystem consists of three components namely finger print scanner device to scan the finger print, finger print analyzer to analyze the obtained finger print, finger print storage system to store the valid finger print. Security control uses fingerprintstorageinterface as an interface to communicate with finger print storage system. The control uses fingerprintanalyzerinterface as an interface to communicate with finger print analyzer to analyze the finger print obtained. The control uses fingerprintscannerinterface as an interface to communicate with finger print scanner device to scan the finger print. It also uses touch screen display to display the necessary prompts.

Retina pattern subsystem consists of three components namely retina pattern scanner device to scan the retina pattern, retina pattern analyzer to analyze the obtained retina pattern, retina pattern storage system to store the valid retina pattern. Security control uses retinapatternstorageinterface as an interface to communicate with retina pattern storage system. The control uses retinapatternanalyzerinterface as an interface to communicate with retina pattern analyzer to analyze the retina pattern obtained. The control uses retinapatternscannerinterface as an interface to communicate with retina pattern scanner device to scan the retina pattern. It also uses touch screen display to display the necessary prompts.

Voice processing subsystem consists of three components namely voice input device to get the voice sample, voice sample analyzer to analyze the obtained voice sample, voice storage system to store the valid voice sample. Security control uses voicestorageinterface as an interface to communicate with voice storage system. The control uses voiceanalyzerinterface as an interface to communicate with voice sample analyzer to analyze the voice sample obtained. The control uses voiceinputdeviceinterface as an interface to communicate with voice input device to get the voice sample. It also uses touch screen display to display the necessary prompts.

Pattern processing subsystem consists of two components namely pattern analyzer to analyze the pattern and pattern storage system to store the pattern. Security control uses patternstorageinterface as an interface to communicate with pattern storage system. The control uses patternanalyzerinterface as an interface to communicate with pattern analyzer to analyze the pattern obtained. It also uses touch screen display to display the necessary prompts.

Image processing subsystem consists of two components namely image analyzer to analyze the image and image storage system to store the selected image. Security control uses imagestorageinterface as an interface to communicate with image storage system. The control uses imagenanalyzerinterface as an interface to communicate with image analyzer to analyze the image selected. It also uses touch screen display to display the necessary prompts.

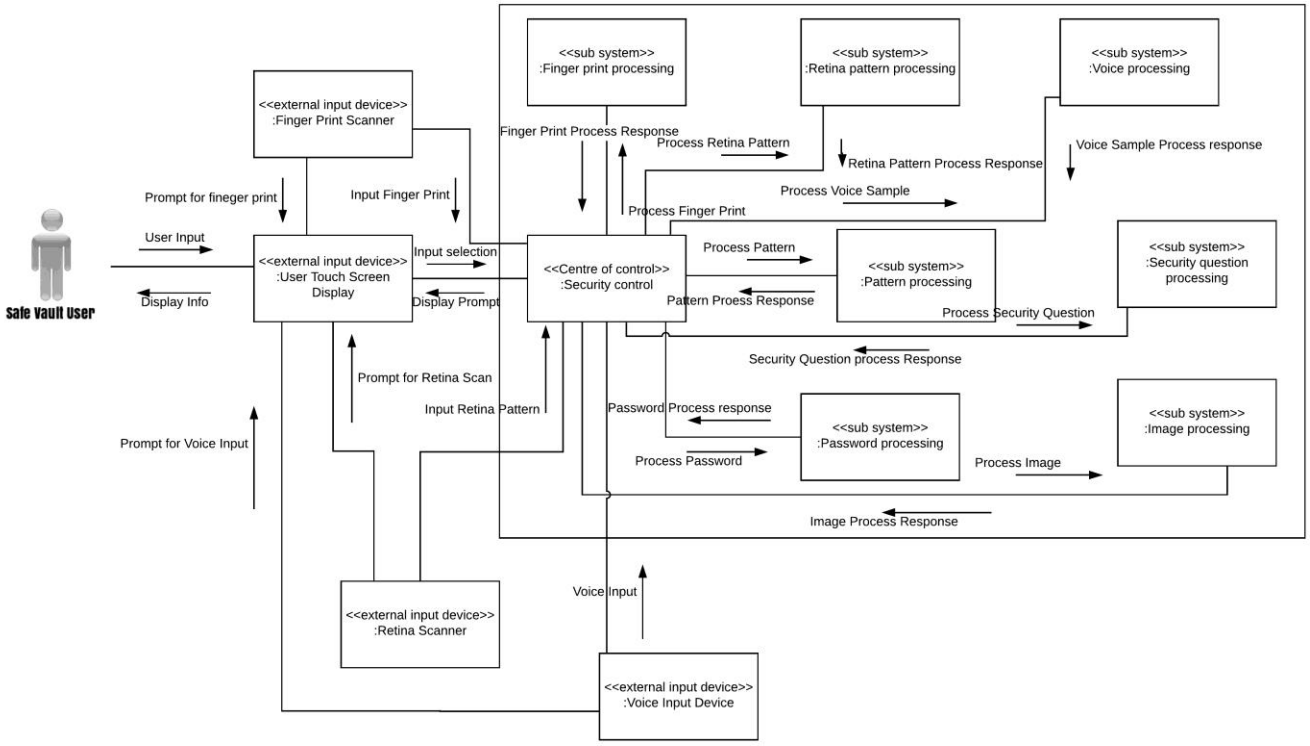
Security Question processing subsystem consists of two components namely security question analyzer to analyze the security answer and security question storage system to store the security answer. Security control uses securityquestionstorageinterface as an interface to communicate with security question storage system. The control uses securityquestionanalyzerinterface as an interface to

communicate with security question analyzer to analyze the answer obtained. It also uses touch screen display to display the necessary prompts.

Password processing subsystem consists of two components namely password analyzer to analyze the password and password storage system to store the password. Security control uses passwordstorageinterface as an interface to communicate with password storage system. The control uses passwordanalyzerinterface as an interface to communicate with password analyzer to analyze the password obtained. It also uses touch screen display to display the necessary prompts.

High level structure diagram:

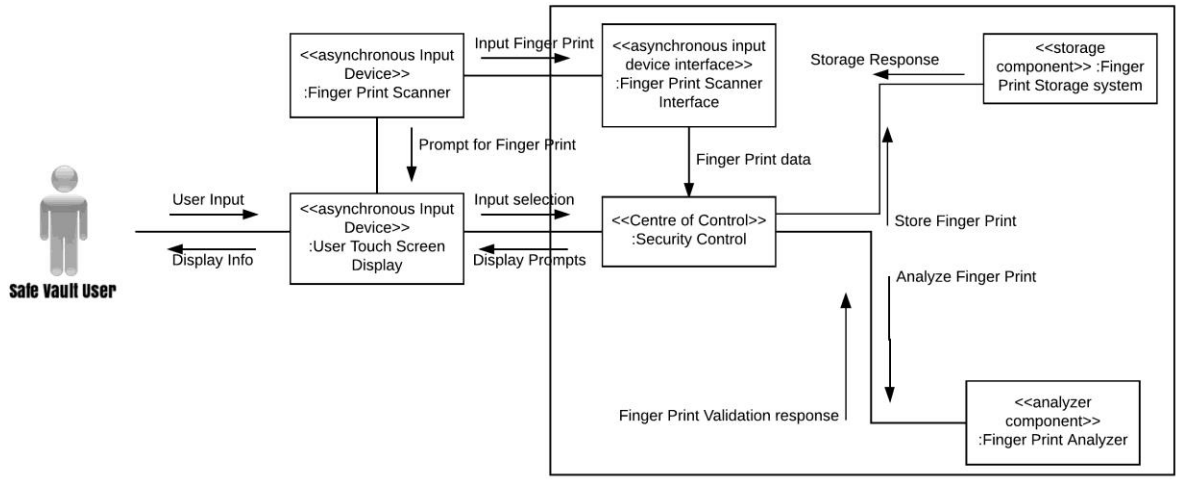
The following diagram shows the high level structure diagram for this system comprising all sub-systems.



In this high level structure diagram, we can see the various subsystems interacting with center of control (security control). We can also see the external devices such as finger print scanner, retina pattern scanner and voice input device interacting with their respective sub-system and the security control. The user interaction is also shown in the image. The request-response message for each subsystem is shown in the diagram which depicts the control and data flow between center of control and the subsystems.

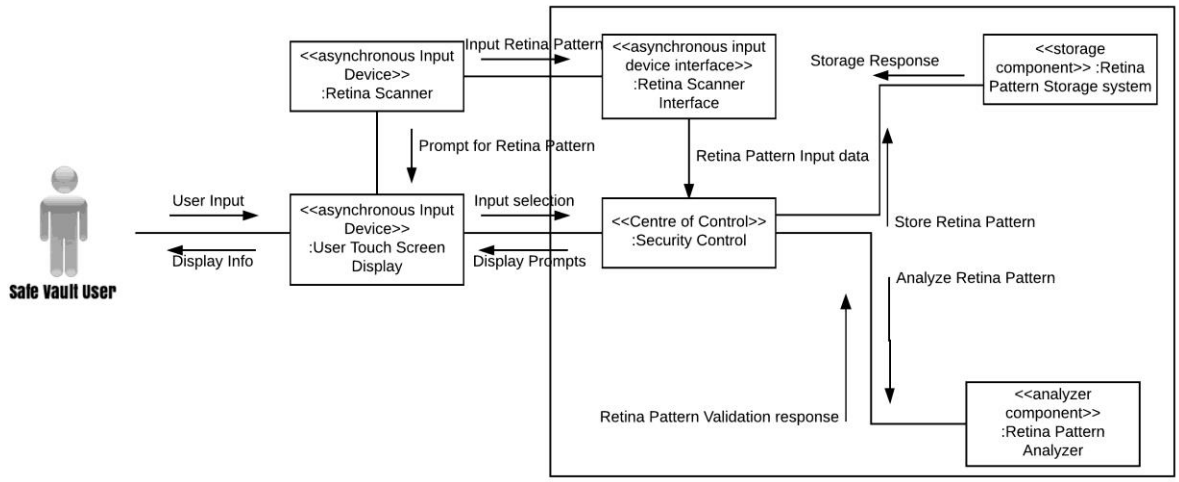
Low level structure diagram for each subsystem:

Finger Print Processing Subsystem



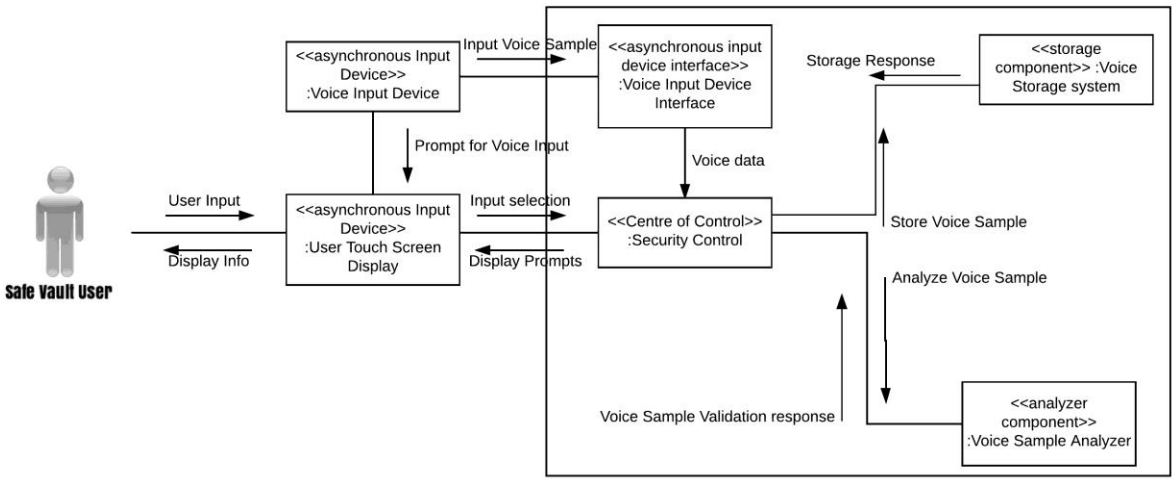
In Finger print processing subsystem, user, finger print scanner, user touch screen display, security control, finger print scanner interface to provide interface between security control and finger print scanner and finger print storage system component, finger print analyzer component are involved. Security control will store the valid finger print in the finger print storage system during configuring security access use case. It will analyze the finger print for validity both in the case of access validation and configuration of the system. User uses finger print scanner to input his finger print and touch screen to interact with the system.

Retina Print Processing Subsystem:



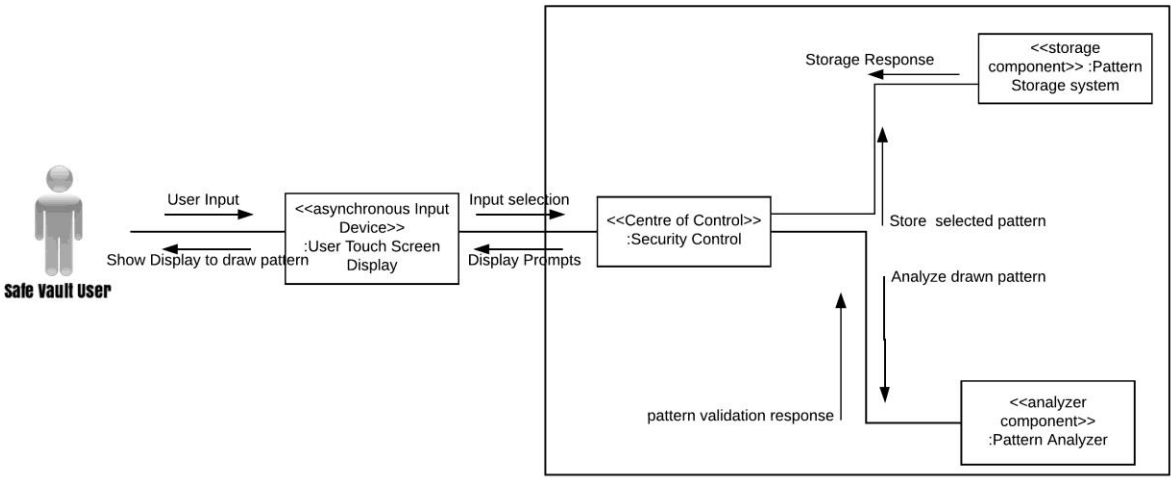
In Retina pattern processing subsystem, user, retina scanner, user touch screen display, security control, retina scanner interface to provide interface between security control and retina scanner device, retina pattern storage system component and retina pattern analyzer component are involved. Security control will store the valid retina pattern in the retina pattern storage system during configuring security access use case. It will analyze the retina pattern for validity both in the case of access validation and configuration of the system. User uses retina scanner to input his retina pattern and touch screen to interact with the system.

Voice Processing Subsystem



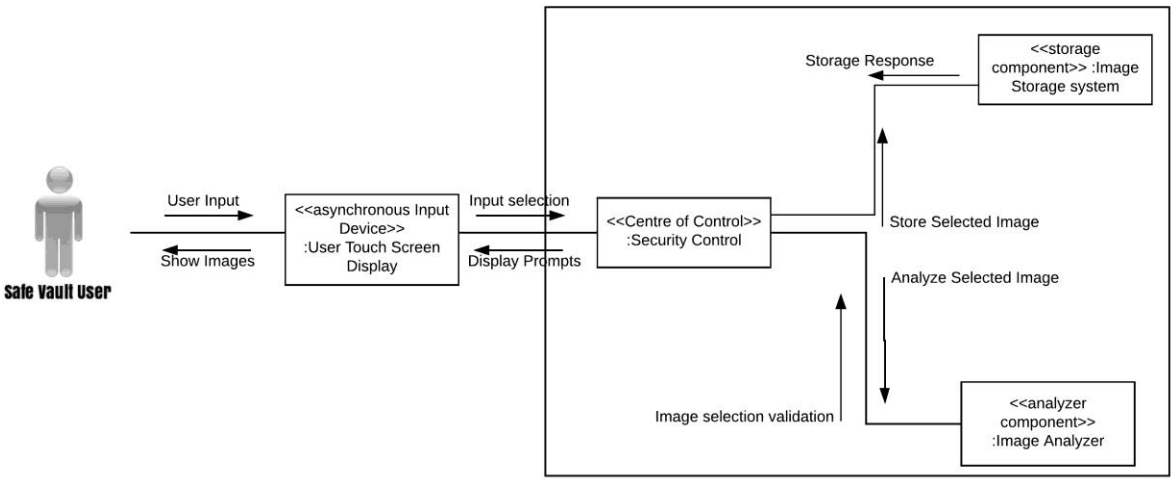
In voice processing subsystem, user, voice input device, user touch screen display, security control, voice input device interface to provide interface between security control and voice input device, voice storage system component and voice sample analyzer component are involved. Security control will store the valid voice sample in the voice storage system during configuring security access use case. It will analyze the voice sample for validity both in the case of access validation and configuration of the system. User uses voice input device to input his voice sample and touch screen to interact with the system.

Pattern Processing Subsystem:



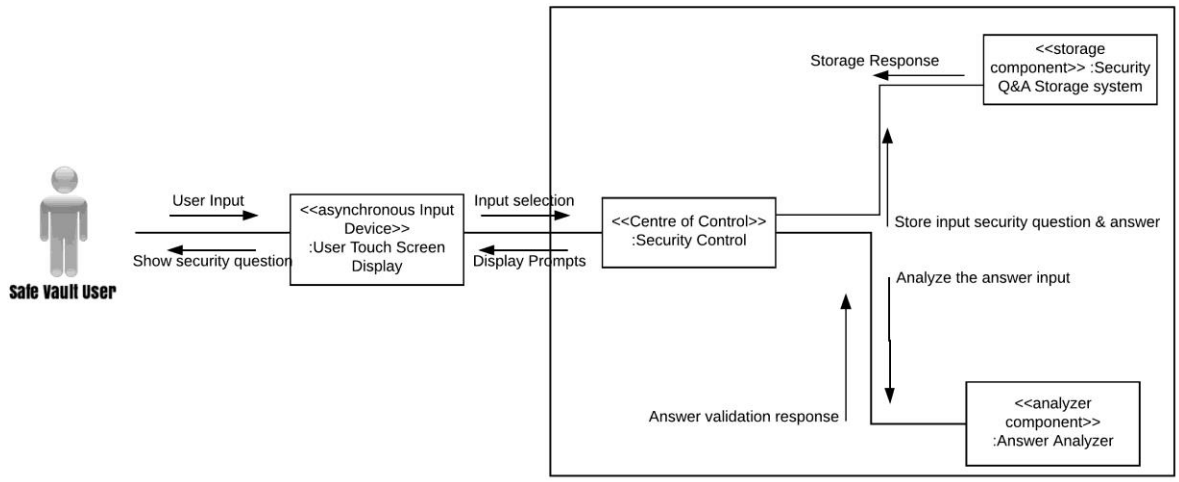
In Pattern processing subsystem, user, user touch screen display, security control, pattern storage system component and pattern analyzer component are involved. Security control will store the valid pattern in the pattern storage system during configuring security access use case. It will analyze the pattern for validity both in the case of access validation and configuration of the system. User uses touch screen to interact with the system.

Image Processing Subsystem:



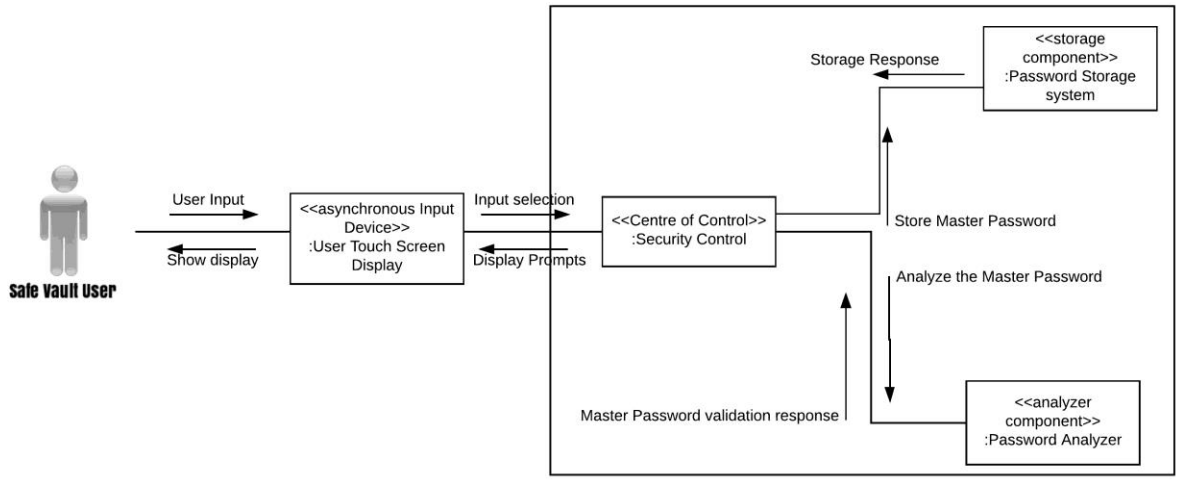
In Image processing subsystem, user, user touch screen display, security control, image storage system component and image analyzer component are involved. Security control will store the valid image selection in the image storage system during configuring security access use case. It will analyze the image for validity both in the case of access validation and configuration of the system. User uses touch screen to interact with the system.

Security Question Processing Subsystem:



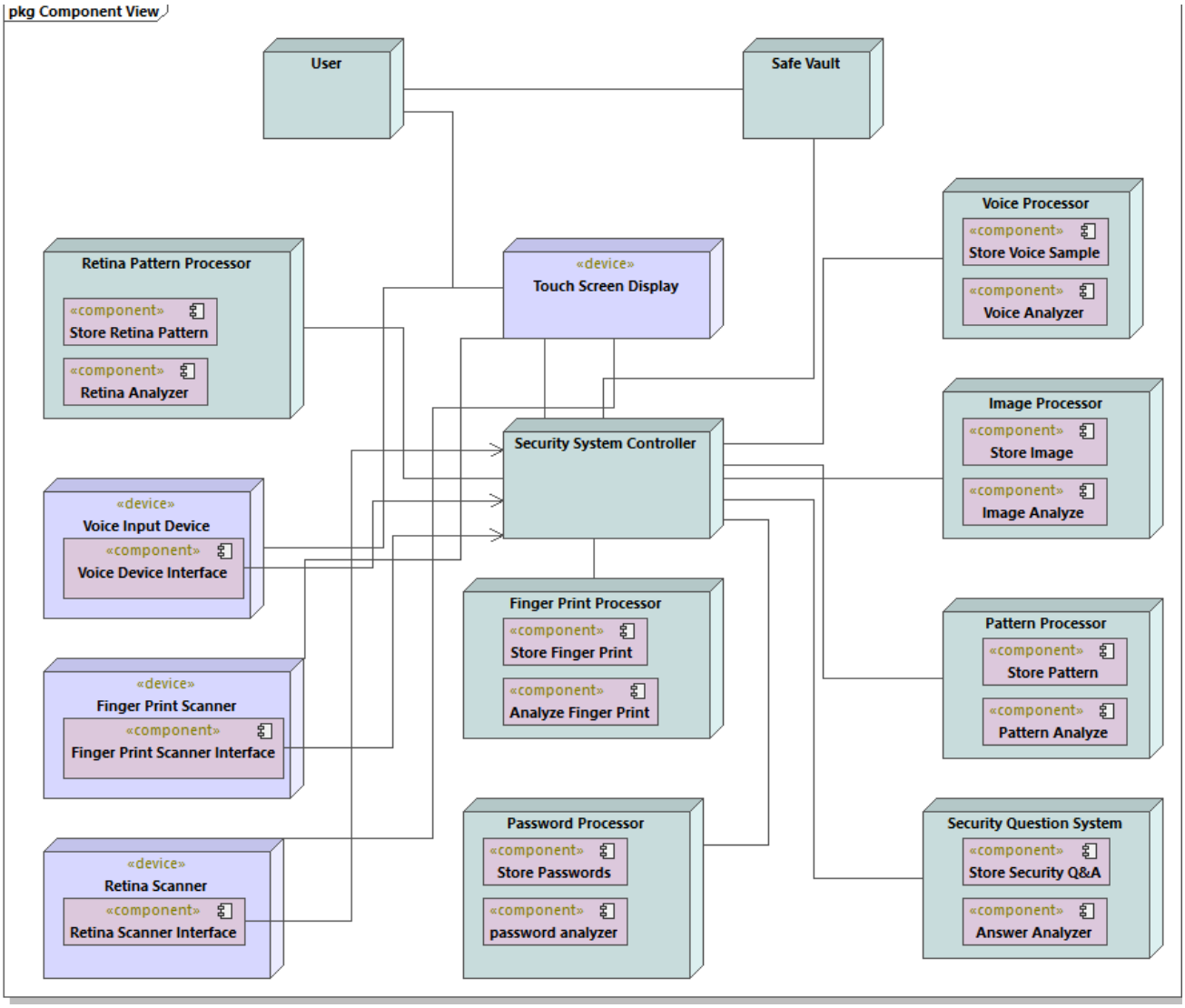
In Security Question processing subsystem, user, user touch screen display, security control, security Q&A storage system component and answer analyzer component are involved. Security control will store the question and answer in the security Q&A storage system during configuring security access use case. It will analyze the answer for validity both in the case of access validation and configuration of the system. User uses touch screen to interact with the system.

Password Processing Subsystem:



In Password processing subsystem, user, user touch screen display, security control, password storage system component and password analyzer component are involved. Security control will store the valid password in the password storage system during configuring security access use case. It will analyze the password for validity both in the case of access validation and configuration of the system. User uses touch screen to interact with the system.

Deployment Diagram:



In deployment diagram, we can see the seven nodes representing the seven subsystems described in structure diagrams. We have two other nodes which represent the user and safe vault system employing the security system. Each subsystem has its respective analyzer and storage component. There are four device nodes which represents the retina scanner, finger print scanner, voice input device and touch screen display. The interaction between nodes and devices can be seen in the diagram.

Conclusion:

Distributed diagram is not discussed in this project as the system involved is a closed environment type and it will be quite infeasible to make the component distributed considering the problem scenario i.e. every component should be present together physically. Thus, Timer based security system has been developed successfully by applying comet methodology. Papyrus and Altova Umodel are the tools that have been used to develop the system modeling.