|  |
| --- |
| LGE |
| Secure Video Call Development |
| Phase1 Final Report |

|  |
| --- |
| Security Specialist Team4 B1C2V3  2023-7-7 |

**Table of Contents**

[1. Introduction 2](#_Toc139386106)

[1.1. Project Overview 2](#_Toc139386107)

[1.2. Project Team 2](#_Toc139386108)

[1.3. Roles and Responsibilities 2](#_Toc139386109)

[2. Project Schedule 3](#_Toc139386110)

[3. Requirement analysis 3](#_Toc139386111)

[3.1. Requirement Analysis Result Overview 3](#_Toc139386112)

[3.2. Functional Requirements Details 4](#_Toc139386113)

[3.3. Non Functional Requirements Details 13](#_Toc139386114)

[3.4. Use Case Scenarios 13](#_Toc139386115)

[4. Test Case Design 18](#_Toc139386116)

[5. Threat analysis 33](#_Toc139386117)

[6. Security requirements & Mitigation 72](#_Toc139386118)

[7. System design 72](#_Toc139386119)

[7.1. Initial Design 72](#_Toc139386120)

[7.2. Design Improvement including Mitigation 73](#_Toc139386121)

[7.3. Backend Server API design 77](#_Toc139386122)

[8. Implementation 79](#_Toc139386123)

[9. Verification 80](#_Toc139386124)

[9.1. Verification Overview 80](#_Toc139386125)

[9.2. Verification Result Detail 81](#_Toc139386126)

[9.3. Verification Result on Security requirements 83](#_Toc139386127)

[9.3.1. Two factor authentication 83](#_Toc139386128)

[9.3.2. Server Authentication & Secure communication 84](#_Toc139386129)

[9.3.3. Storing log file to the file system 84](#_Toc139386130)

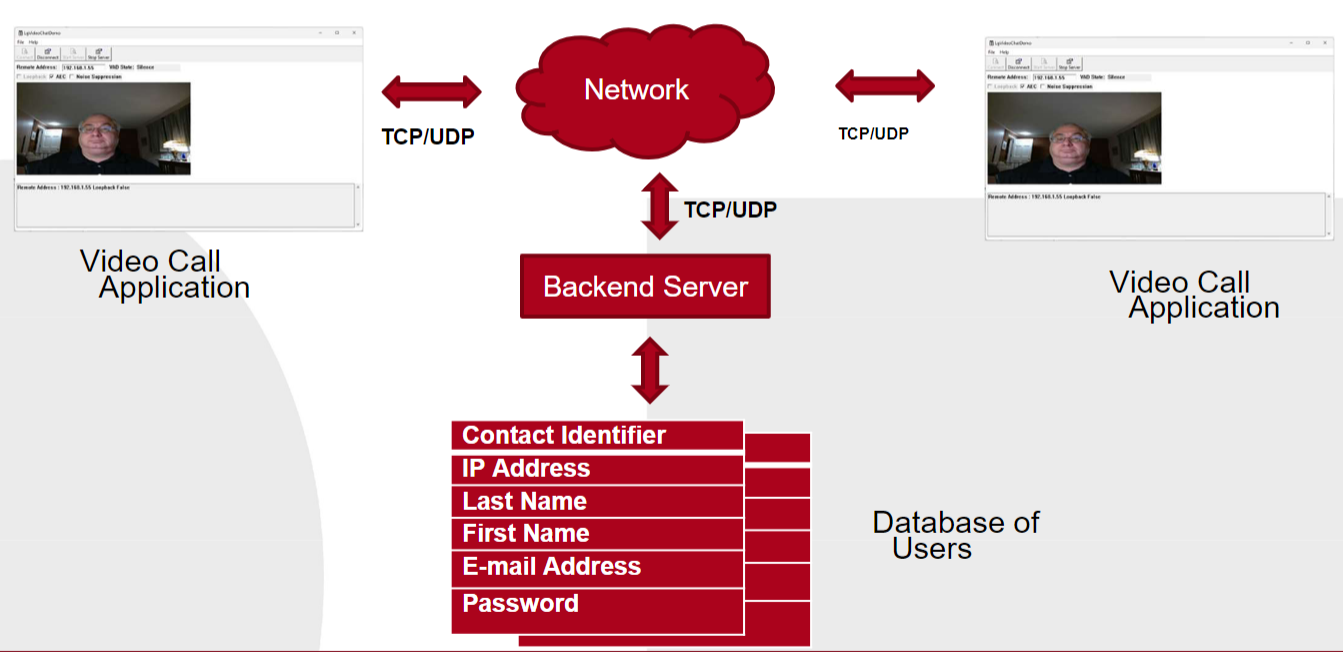
[10. Lessons Learned 84](#_Toc139386131)

# Introduction

## Project Overview

**System overview**

* Video Call Application for both business and personal users
* Video Call Communication over the Network
* User registration and login function with two factor authentication
* **Current design needs to be improved in terms of security**



## 1.2. Project Team

Team Name : B1C2V3

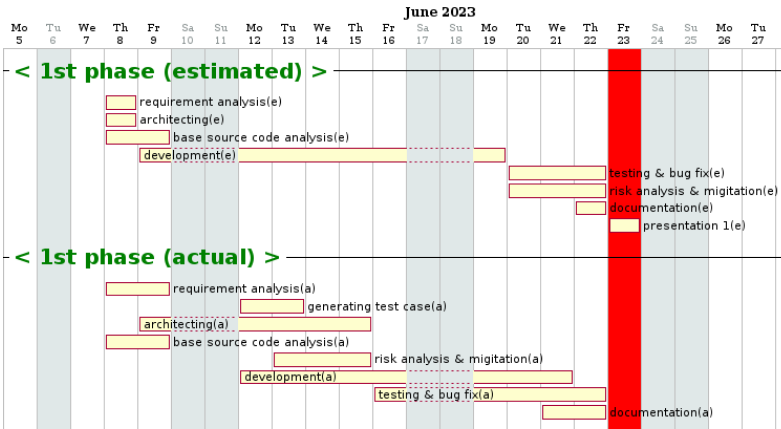
(1 member from BS company, 2 members from CTO, 3 members from VS company)

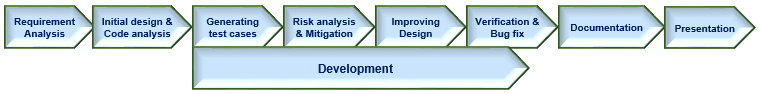
Team logo : 

## 1.3. Roles and Responsibilities

|  |  |
| --- | --- |
| Name | Responsibilities |
| Jongoh Ha | Team leader |
| Chanhun Seung | Threat Analyst & Architect |
| Youngjin Kim | Requirement manager & Test manager |
| Hongjae Lim | Application developer |
| Minji Tae | Application developer |
| Truong Quang Viet | Backend Server developer |

# Project Schedule





# Requirement analysis

## Requirement Analysis Result Overview

|  |  |  |
| --- | --- | --- |
| Functional Requirement | New user registration | 11 |
| Login | 8 |
| User email update | 8 |
| Periodic password reset | 10 |
| Lockout due to incorrect password | 13 |
| Reset password | 7 |
| Unique ID | 1 |
| Contact list | 2 |
| Call | 4 |
| Connection | 2 |
| Notice | 2 |
| Disconnect | 2 |
| Activation | 1 |
| Communication method | 1 |
| Non Functional Requirement | Performance | 1 |
| Authentication | 2 |
| Communication privacy | 1 |
| Non repudiation | 1 |
| Reliability | 1 |
| Total |  | 78 |

* Number of given requirements : 19  
  (functional : 14, non functional : 5)
* Analyzed given requirements throughs **team workshop** and **mentor meeting**
* Requirement manager derived **78 system requirements** through additional analysis

## Functional Requirements Details

Table . Functional Requirement Analysis Result

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Req. ID | Req. Name | Sub Req. ID | Description | PR ID | Test ID | Implemented by |
| FR01 | new user registration | FR01REG01 | The system shall provide new user registration form that captures essential information such as first name, last name, email address, OTP and password. | PR01B | TC001 | App |
|  |  | FR01REG02 | The system shall implement validation to ensure the uniqueness of email addresses to prevent multiple users from registering with the same credentials. | PR01 | TC002, TC003 | Backend |
|  |  | FR01REG03 | The system shall send a verification email to the user's provided email address upon registration to confirm their ownership and prevent misuse. | PR01F | TC002, TC003 | Backend |
|  |  | FR01REG04 | The system shall include an OTP in the email to be sent to verify their account. | PR01B | TC007 | Backend |
|  |  | FR01REG05 | The system shall implement a mechanism to handle expired or revoked verification OTP |  | TC006 | Backend |
|  |  | FR01REG06 | Passwords must be a minimum of 10 characters long and include one number and one special character. | PR01A | TC004 | Backend |
|  |  | FR01REG07 | Passwords must be confirmed through re-type. |  | TC005 | Backend + App |
|  |  | FR01REG08 | The system shall hash and salt the passwords before storing them in the database to enhance security. |  |  | Backend |
|  |  | FR01REG09 | The system shall provide meaningful error messages and validation feedback to users during the registration process to assist them in resolving any issues they encounter. |  | TC008 | Backend |
|  |  | FR01REG10 | The system shall implement error logging and monitoring to track and investigate any registration-related errors or anomalies. |  | TC008 | Backend |
|  |  | FR01REG11 | The system shall implement CAPTCHA or other anti-bot mechanisms to prevent automated registrations. ( Optional ) |  | TC009 |  |
| FR02 | Login | FR02LOG01 | The user shall provide the system their email address, password and OTP. | PR01A, PR01B | TC010 | App |
|  |  | FR02LOG02 | The email address should be in a standard format. (e.g., "[example@example.com](mailto:example@example.com)"). | PR01A | TC011 | Backend + App |
|  |  | FR02LOG03 | The password information must be masked and show | PR01A |  | App |
|  |  | FR02LOG04 | The system should provide appropriate error messages or notifications to the user if there are any issues with the provided email address or password. |  | TC012 | Backend + App |
|  |  | FR02LOG05 | If email and password are corrected, the user can request OTP | PR01B | TC013 | Backend + App |
|  |  | FR02LOG06 | The OTP will be sent to the user's email. | PR01B | TC014,TC015 | Backend |
|  |  | FR02LOG07 | The OTP must be 6 characters long and consist of numbers only. | PR01B | TC014,TC015 | Backend |
|  |  | FR02LOG08 | The system should provide appropriate error messages or notifications to the user if there are any issues with the OTP. | PR01B | TC016 | Backend + App |
| FR03 | user email update | FR03UPD01 | Only authorized users should be able to access the functionality to change their email address. | PR01E | TC017 | Backend |
|  |  | FR03UPD02 | Before allowing users to change their email address, the system should authenticate their identity to ensure they are the legitimate account holders using password. | PR01E | TC018 | Backend |
|  |  | FR03UPD03 | The system should validate the user-provided email address to ensure it follows the correct format. | PR01E | TC019 | Backend + App |
|  |  | FR03UPD04 | The system should send a verification OTP to the new email address provided by the user. | PR01E | TC020 | Backend |
|  |  | FR03UPD05 | The system should require the user to confirm the change by entering the OTP within a specified timeframe | PR01E | TC020 | Backend |
|  |  | FR03UPD06 | The system should implement proper error handling mechanisms to handle scenarios such as invalid email addresses, database failures, network errors, or other exceptional cases. | PR01E | TC021 | Backend |
|  |  | FR03UPD07 | Ensure the audit trail is securely stored and accessible only to authorized personnel for monitoring, auditing, and investigating purposes. | PR01E | TC021 | Backend |
|  |  | FR03UPD08 | The system should notify users via their existing email address when a change to their email address is requested or successfully completed. | PR01E | TC017 | Backend |
| FR04 | Periodic PW Reset | FR04PWRST01 | The system shall store the date and time of the user's last password reset | PR01C |  | Backend |
|  |  | FR04PWRST02 | The system shall enforce a maximum password lifetime of one month (30 days) | PR01C | TC022 | Backend |
|  |  | FR04PWRST03 | The system shall compare the current date with the user's last password reset date to determine if a password reset is required | PR01C | TC022 | Backend |
|  |  | FR04PWRST04 | If the time since the last password reset exceeds one month, the system shall prompt the user to reset their password | PR01C | TC023 | Backend |
|  |  | FR04PWRST05 | The system shall display a notification to the user when their password is due for a reset | PR01C | TC023,TC024 | App |
|  |  | FR04PWRST06 | The system shall validate and confirm the new password entered by the user to ensure accuracy | PR01C | TC025 | Backend + App |
|  |  | FR04PWRST07 | The system shall log the date and time of the password reset for auditing and security purposes | PR01C | TC027 | Backend |
|  |  | FR04PWRST08 | The system shall send a notification email to the user after a successful password reset, confirming the password change | PR01C | TC026 | Backend |
|  |  | FR04PWRST09 | The system shall store the history of the user's previous passwords to prevent reuse of the same or similar passwords within a specified period (e.g., the last five passwords) | PR01C | TC028,TC029 | Backend |
|  |  | FR04PWRST10 | The system shall provide an option for users to contact support if they encounter any issues during the password reset process or have concerns about their password security | PR01C | TC027 | Backend + App |
| FR05 | Lockout due to an incorrect password | FR05LOCK01 | The system shall track the number of failed login attempts for each user. | PR01D | TC031 | Backend |
|  |  | FR05LOCK02 | The system shall increment the failed login attempt count by one each time a user enters an incorrect password. | PR01D | TC030 | Backend |
|  |  | FR05LOCK03 | The system shall reset the failed login attempt count to zero if the user successfully logs in. | PR01D | TC031 | Backend |
|  |  | FR05LOCK04 | The system shall lock a user's account if the failed login attempt count exceeds a predefined threshold (e.g., three). | PR01D | TC032 | Backend |
|  |  | FR05LOCK05 | The system shall enforce a lockout duration of one hour for a locked account | PR01D | TC033 | Backend |
|  |  | FR05LOCK06 | The system shall display an appropriate error message to the user when their account is locked due to excessive failed login attempts. | PR01D | TC035 | Backend + App |
|  |  | FR05LOCK07 | The system shall prevent a locked account from being accessed during the lockout duration, regardless of the password entered | PR01D | TC033 | Backend |
|  |  | FR05LOCK08 | The system shall display a countdown timer indicating the remaining lockout duration for the user | PR01D | TC033 | App |
|  |  | FR05LOCK09 | The system shall automatically unlock the user's account after the lockout duration has elapsed | PR01D | TC034 | Backend |
|  |  | FR05LOCK10 | The system shall notify the user via email when their account is locked due to excessive failed login attempts | PR01D | TC035 | Backend |
|  |  | FR05LOCK11 | The system shall include a link in the email notification for the user to contact support if they believe their account has been locked incorrectly or for any other account-related issues. | PR01D | TC035 | Backend |
|  |  | FR05LOCK12 | The system shall log all account lockout events for auditing and security purposes | PR01D | TC032 | Backend |
|  |  | FR05LOCK13 | The system shall provide an option for users to reset their password during the account lockout period using the password recovery functionality. | PR01D | TC036 | Backend + App |
| ~~FR06~~ | ~~Reset PW~~ | ~~FR06PWRST01~~ | ~~The system shall provide a form for users to initiate password recovery.~~ | PR01F | TC037,TC039 | App |
|  |  | ~~FR06PWRST02~~ | ~~The system shall show the user to enter their registered email address.~~ | PR01F | TC037 | App |
|  |  | ~~FR06PWRST03~~ | ~~The system shall validate the entered email address and verify its existence in the user database.~~ | PR01F | TC037,TC038 | Backend |
|  |  | ~~FR06PWRST04~~ | ~~If the email address is valid and registered, the system shall generate a temporary password and send it to the user's email address.~~ | PR01F | TC037,TC038,  TC040 | Backend |
|  |  | ~~FR06PWRST05~~ | ~~The system shall provide a secure password reset form where the user can enter a new password after the user successfully login using the temporary password~~ | PR01F | TC039 | Backend + App |
|  |  | ~~FR06PWRST06~~ | ~~Upon successful password reset, the system shall notify the user via email that their password has been changed.~~ | PR01F | TC039 | Backend |
|  |  | ~~FR06PWRST07~~ | ~~The system shall log all password recovery and reset activities for auditing and security purposes.~~ | PR01F | TC041~TC043 | Backend |
| FR07 | Unique ID | FR07UID01 | After successful registration the system shall assign the user a unique contact identifier. | PR02 | TC044 | Backend |
| FR08 | Contact list | FR08CTT01 | The system shall provide a contact list that associates a person with their contact identifier (last name, first name, e-mail, contact identifier). | PR03 | TC044 | Backend |
|  |  | FR08CTT02 | When a contact is associated with a contact identifier the VoIP application shall display the contact’s name instead of the contact identifier. | PR03 | TC045 | App |
| FR09 | call | FR09CALL01 | The system shall provide the ability to initiate a call using a contact identifier or the contacts list. | PR04 | TC046 | App |
|  |  | FR09CALL02 | The system shall maintain a log of call activities, including call start time, duration, participants, and call outcome (answered, busy, or rejected). | PR04 | TC046 | Backend |
|  |  | FR09CALL03 | Provide a call history feature that allows users to view and review past calls, including details like participants, timestamps, and call duration. | PR04 | TC047 | App |
|  |  | FR09CALL04 | During the call initiation, the user shall be presented with call status and outcome (answered, busy or rejected). | PR04 | TC048 | App |
| FR10 | connection | FR10CON01 | The system shall provide the ability to accept or reject calls while not in a call. | PR05 | TC050,TC051 | App |
|  |  | FR10CON02 | Application shall show the caller’s contact identifier or contact name during an incoming call. | PR05 | TC050 | App |
| FR11 | notice | FR11NOTI01 | The system shall notify the user of missed calls, in case of the call was not accepted. | PR06 | TC051,TC0525 | App |
|  |  | FR11NOTI02 | The system shall notify the user of missed calls, when the called entity was in another call. | PR06 | TC053 | App |
| FR12 | disconnect | FR12DISC01 | Provide the ability to terminate a call at any time while in a call. | PR04,PR07 | TC049 | App |
|  |  | FR12DISC01 | If a call is terminated by one user, the other caller shall be notified. | PR07 | TC054 | App |
| FR13 | Activation | FR13ACT01 | Application shall be brought to the foreground during an incoming call. | PR08 | TC055 | App |
| FR14 | Communication methods | FR14CMM01 | This application is a point-to-point communication system. That is, each end point of the call should function as both a server and a client. | PR09 | TC056 | App |

## Non Functional Requirements Details

Table . Non Functional Requirement Analysis Result

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Req. ID | Req. Name | Func ID | Func Name | Description | PR ID |  |
| NFR01 | Performance | NFR01\_PERF01 | Real time communication | The system must deliver call video/audio as close to real time as possible. | PR10 |  |
| NFR02 | Authentication | NFR02\_AUTH01 |  | The system must use two factor authentication for sign on and user credentials must be protected. | PR11 |  |
|  |  | NFR02\_AUTH02 |  | Lost or compromised credentials must be handled in a reasonable way. | PR11 |  |
| NFR03 | communication privacy | NFR03\_PRI01 | Privating communication | The system must ensure that calls remain private. No intermediary should be able to snoop or spy on an ongoing call. | PR12 |  |
| NFR04 | nonrepudiation | NFR04\_NREP01 |  | Users should be confident that the entity they are on a call with is the one that they believe it is. | PR13 |  |
| NFR05 | reliability | NFR05\_REL01 |  | The system must ensure that calls are reliable. The system should recover from networking errors and dropped calls as soon as possible. The goal is to maintain a secure, performant connection at all costs. | PR14 |  |

## Use Case Scenarios

**FR01 New User Registration**

Table . Use case scenarios

|  |  |
| --- | --- |
| Req ID | FR01 |
| Title | New User Registration |
| Primary Actor | User |
| Pre-conditions | * The user must have access to the registration form provided by the system. * The system must be operational and able to handle registration requests. * The user must have a valid email address to receive the verification email. * The user must have a secure internet connection to access the registration form and receive the verification email. * The database server must be accessible and able to store user data. |
| Scenario | 1. User opens the registration form of the system. 2. System presents the registration form to the user, including fields for first name, last name, email address, OTP, and password. 3. User enters their registration information. 4. System validates the uniqueness of the email address. 5. If the email address is already registered, the system displays an error message to the user. 6. If the email address is unique, the system generates a unique identifier for the user. 7. System sends a verification email to the user's provided email address, including an OTP. 8. User checks their email and retrieves the OTP. 9. User enters the OTP into the registration form. 10. System validates the OTP and checks for expiration or revocation. 11. If the OTP is invalid, expired, or revoked, the system displays an error message to the user. 12. If the OTP is valid, the system enforces password requirements. 13. User enters and confirms their password, ensuring it meets the requirements. 14. System hashes and salts the password for secure storage. 15. System stores the user's registration data in the database. 16. System displays a success message to the user, confirming their registration. 17. User can now log in to the system using their registered email address and password. |
| Post-conditions | * Upon successful registration, the user's information is stored securely in the database. * The user receives a verification email containing an OTP to verify their account. * If the OTP is validated successfully, the user is considered registered and can proceed with logging into the system. * The user can now access the system using their registered email address and password. |
| Alternate Flow | 1. User opens the registration form of the system. 2. System presents the registration form to the user, including fields for first name, last name, email address, OTP, and password. 3. User enters their registration information. 4. System validates the uniqueness of the email address. 5. If the email address is already registered, the system displays an error message to the user. 6. If the email address is unique, the system encounters an error while generating a unique identifier. 7. System displays an error message to the user, indicating the problem with generating a unique identifier. 8. User can choose to retry the registration process or contact support for assistance. 9. If the user chooses to retry, the process continues from Step 1. 10. If the user chooses to contact support, the process is temporarily halted until the issue is resolved. 11. Once the issue is resolved, the user can proceed with the registration process from the beginning. |

**FR02 Login**

|  |  |
| --- | --- |
| Req ID | FR02 |
| Title | Login |
| Primary Actor | User |
| Pre-conditions | * The user must have a registered account with the system. * The user must have a valid email address and password. * The user must have access to their registered email account. * The system must be operational and accessible. |
| Scenario | 1. User opens the login page of the system. 2. System presents the login form to the user, including fields for email address, password, and OTP. 3. User enters their email address and password. 4. System validates the email address and password format. 5. If the email address or password is invalid, the system displays an error message to the user. 6. If the email address and password are valid, the user can request an OTP. 7. User clicks the "Request OTP" button. 8. System generates an OTP and sends it to the user's registered email address. 9. User checks their email and retrieves the OTP. 10. User enters the OTP into the login form. 11. System validates the OTP format and checks for expiration. 12. If the OTP is invalid or expired, the system displays an error message to the user. 13. If the OTP is valid, the system authenticates the user. 14. System logs the user into the system and grants access to the authorized features. 15. System displays a success message to the user, confirming their login. 16. User can now interact with the system and perform the desired actions. |
| Post-conditions | * The user is successfully logged into the system. * The user has access to the authorized features and functionalities. * The system tracks the user's session and activity. * The user can perform actions within their authorized scope. * If the user encounters any issues during the login process, appropriate error messages are displayed, and the user is guided to resolve the issues. |
| Alternate Flow | 1. User opens the login page of the system. 2. System presents the login form to the user, including fields for email address, password, and OTP. 3. User enters their email address and password. 4. System validates the email address and password format. 5. If the email address or password is invalid, the system displays an error message to the user. 6. If the email address and password are valid, the user can request an OTP. 7. User clicks the "Request OTP" button. 8. System encounters an issue sending the OTP to the user's email address. 9. System displays an error message to the user, indicating the problem with the email delivery. 10. User can choose to retry the OTP request or contact support for assistance. 11. If the user chooses to retry, the process continues from Step 7. 12. If the user chooses to contact support, the process is temporarily halted until the issue is resolved. 13. Once the issue is resolved, the user can proceed with the login process from the beginning. |

**FR03 User Email Update**

|  |  |
| --- | --- |
| Req ID | FR03 |
| Title | User Email Update |
| Primary Actor | User |
| Pre-conditions | * The user must be an authorized user with access to the email update functionality. * The user must have a valid account and be logged into the system. * The user must have an existing email address associated with their account. * The user must have a secure internet connection to access the email update functionality. * The system must be operational and able to handle email update requests. |
| Scenario | 1. User initiates the email update process. 2. System authenticates the user's identity by requesting their password. 3. User enters their password. 4. System validates the password and confirms the user's identity. 5. System presents the email update form to the user. 6. User enters the new email address they wish to update to. 7. System validates the new email address format. 8. If the new email address is invalid, the system displays an error message to the user. 9. If the new email address is valid, the system sends a verification OTP to the new email address. 10. System displays a success message indicating that the verification OTP has been sent. 11. User checks their new email address and retrieves the OTP. 12. User enters the OTP within the specified timeframe. 13. System verifies the OTP and confirms the email address change. 14. If the OTP is incorrect or expired, the system displays an error message to the user. 15. If the OTP is correct and within the specified timeframe, the system updates the user's email address. 16. System securely stores the audit trail of the email address change. 17. System sends a notification email to the user's existing email address, informing them of the email address change. 18. System displays a success message to the user, confirming the email address change. |
| Post-conditions | * The user's email address is successfully updated in the system. * The user receives a notification email informing them of the email address change. * The user can now use the new email address for authentication and communication. * If the user encounters any issues during the email update process, appropriate error messages are displayed, and the user is guided to resolve them. |
| Alternate Flow | 1. User initiates the email update process. 2. System authenticates the user's identity by requesting their password. 3. User enters their password. 4. System validates the password and confirms the user's identity. 5. System presents the email update form to the user. 6. User enters the new email address they wish to update to. 7. System validates the new email address format. 8. If the new email address is invalid, the system displays an error message to the user. 9. If the new email address is valid, the system encounters an error while sending the verification OTP. 10. System displays an error message to the user, indicating the problem with sending the verification OTP. 11. User can choose to retry the email update process or contact support for assistance. 12. If the user chooses to retry, the process continues from Step 1. 13. If the user chooses to contact support, the process is temporarily halted until the issue is resolved. 14. Once the issue is resolved, the user can proceed with the email update process from the beginning. |

**FR04 Periodic Password Reset**

|  |  |
| --- | --- |
| Req ID | FR04 |
| Title | Periodic Password Reset |
| Primary Actor | User |
| Pre-conditions | * User is logged in. * User's password has expired. |
| Scenario | 1. System prompts the user to enter a new password. 2. User enters a new password. 3. System validates the new password. 4. System updates the user's password in the system's database. 5. System logs the date and time of the password reset. 6. System sends a confirmation email to the user, confirming the password change. |
| Post-conditions | * User's password is successfully reset. * User receives a confirmation email. |
| Alternate Flow | 1. N/A |

**FR05 Incorrect Password Lock**

|  |  |
| --- | --- |
| Req ID | FR05 |
| Title | Incorrect Password Lock |
| Primary Actor | User |
| Pre-conditions | * User has a registered account |
| Scenario | 1. User enters their username and password. 2. System verifies the entered credentials. 3. If the credentials are valid:    1. System resets the failed login attempt count to zero.    2. User is successfully logged in. 4. If the credentials are invalid:    1. System increments the failed login attempt count by one for the user.    2. If the failed login attempt count exceeds the predefined threshold:       1. System locks the user's account.       2. System displays an error message to the user indicating that their account is locked due to excessive failed login attempts. |
| Post-conditions | * User is successfully logged in. * User's account is locked if the failed login attempt threshold is exceeded. * User receives an error message if their account is locked |
| Alternate Flow | 4a. If the user's account is locked:   1. System displays an error message indicating that the account is locked. 2. System displays a countdown timer indicating the remaining lockout duration for the user. 3. User cannot access the account during the lockout duration, regardless of the password entered. |

# Test Case Design

Test cases are generated based on functional requirements in previous chapter.

**Sign-Up**

Test Case 1: Successful Registration

|  |  |
| --- | --- |
| Test Case ID | TC001 |
| Title | Successful Registration |
| Pre-conditions | The Sign-Up form is accessible and all required fields are provided. |
| Sequence | Enter a unique email address.  Click “Duplicate Check” Button  Enter a valid password.  Confirm the password by re-typing it.  Enter a valid first name.  Enter a valid last name. |
| Input Values | Email Address: [john.doe@example.com](mailto:john.doe@example.com)  Password: Abcd1234!@#$  Confirm Password: Abcd1234!@#$  First Name: john  Last Name: doe |
| Expected Result | User account is created successfully.  Verification email is sent to the provided email address.  Success message displayed. |
| Post-conditions | The user's account is registered and pending verification. |

Test Case 2: Invalid Email Address

|  |  |
| --- | --- |
| Test Case ID | TC002 |
| Title | Invalid Email Address |
| Pre-conditions | The Sign-Up form is accessible. |
| Sequence | Enter an invalid email address format.  Click “Duplicate Check” |
| Input Values | Email Address: [john.doe@example.com](mailto:john.doe@example.com) |
| Expected Result | Error message displayed indicating invalid email address format. |
| Post-conditions | The system show to correct the email address format. |

Test Case 3: Existing Email Address

|  |  |
| --- | --- |
| Test Case ID | TC003 |
| Title | Existing Email Address |
| Pre-conditions | The Sign-Up form is accessible. |
| Sequence | Enter an email address that is already registered in the system. |
| Input Values | Email Address: [john.doe@example.com](mailto:john.doe@example.com) |
| Expected Result | Error message displayed indicating that the email address is already in use. |
| Post-conditions | The user is prompted to provide a different email address. |

Test Case 4: Weak Password

|  |  |
| --- | --- |
| Test Case ID | TC004 |
| Title | Weak Password |
| Pre-conditions | The Sign-Up form is accessible. |
| Sequence | Enter a unique email address.  Enter a weak password that does not meet the complexity requirements.  Confirm the password by re-typing it.  Enter a first name.  Enter a last name. |
| Input Values | Email Address: [john.doe@example.com](mailto:john.doe@example.com)  Password: password123  Confirm Password: password123  First Name: John  Last Name: Doe |
| Expected Result | Error message displayed indicating password complexity requirements not met. |
| Post-conditions | The user is prompted to provide a stronger password. |

Test Case 5: Password Mismatch

|  |  |
| --- | --- |
| Test Case ID | TC005 |
| Title | Password Mismatch |
| Pre-conditions | The Sign-Up form is accessible. |
| Sequence | Enter a unique email address.  Enter a valid password.  Confirm the password by re-typing it with a different value.  Enter a first name.  Enter a last name. |
| Input Values | Email Address: john.doe@example.com  Password: Abcd1234!@#$  Confirm Password: DifferentPassword123  First Name: John  Last Name: Doe |
| Expected Result | Error message displayed indicating that the passwords do not match. |
| Post-conditions | The user is prompted to re-enter the password correctly. |

Test Case 8: Error Logging

|  |  |
| --- | --- |
| Test Case ID | TC008 |
| Title | Successful Verification |
| Pre-conditions | The Sign-Up process encounters an internal error. |
| Sequence | Submit the Sign-Up form, triggering an internal error. |
| Input Values | N/A |
| Expected Result | Error is logged.  Error notification is generated for further investigation. |
| Post-conditions | Error is flagged for investigation and resolution. |

**Sign-In**

Test Case 10: Successful Sign-In

|  |  |
| --- | --- |
| Test Case ID | TC010 |
| Title | Successful Sign-In |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter a valid email address.  Enter a valid password.  Click on the “Create OTP” button.  Enter a OTP passed via email |
| Input Values | Email Address: john.doe@example.com  Password: Abcd1234!@#$ |
| Expected Result | User is successfully logged in |
| Post-conditions | The user is logged in and has access to their account. |

Test Case 11: Invalid Email Address

|  |  |
| --- | --- |
| Test Case ID | TC011 |
| Title | Invalid Email Address |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter an invalid email address format.  Enter a valid password.  Click on the "Create OTP" button. |
| Input Values | Email Address: invalidemail  Password: Abcd1234!@#$ |
| Expected Result | Error message displayed indicating an invalid email address format. |
| Post-conditions | The user is prompted to correct the email address format. |

Test Case 12: Incorrect Password

|  |  |
| --- | --- |
| Test Case ID | TC012 |
| Title | Incorrect Password |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter a valid email address.  Enter an incorrect password.  Click on the "Create OTP" button. |
| Input Values | Email Address: john.doe@example.com  Password: IncorrectPassword123 |
| Expected Result | Error message displayed indicating an incorrect password. |
| Post-conditions | The user is prompted to enter the correct password. |

Test Case 13: Request OTP

|  |  |
| --- | --- |
| Test Case ID | TC013 |
| Title | Request OTP |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter a valid email address.  Enter a valid password.  Click on the "Create OTP" button. |
| Input Values | Email Address: john.doe@example.com  Password: Abcd1234!@#$ |
| Expected Result | User is prompted to enter the OTP received via email.  Start OTP time count down during a minute |
| Post-conditions | The user is prompted to enter the OTP for verification. |

Test Case 14: Invalid OTP

|  |  |
| --- | --- |
| Test Case ID | TC014 |
| Title | Invalid OTP |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter a valid email address.  Enter a valid password.  Enter an invalid OTP.  Click on the "Verify OTP" button. |
| Input Values | Email Address: john.doe@example.com  Password: Abcd1234!@#$  OTP: InvalidOTP |
| Expected Result | Error message displayed indicating an invalid OTP. |
| Post-conditions | The user is prompted to enter the correct OTP. |

Test Case 15: Successful OTP Verification

|  |  |
| --- | --- |
| Test Case ID | TC015 |
| Title | Successful OTP Verification |
| Pre-conditions | The Sign-In form is accessible. |
| Sequence | Enter a valid email address.  Enter a valid password.  Enter the correct OTP received via email.  Click on the "Confirm" button. |
| Input Values | Email Address: john.doe@example.com  Password: Abcd1234!@#$  OTP: ValidOTP |
| Expected Result | User is successfully verified and logged in. |
| Post-conditions | The user is logged in and has access to their account. |

Test Case 16: Error Logging

|  |  |
| --- | --- |
| Test Case ID | TC016 |
| Title | Error Logging |
| Pre-conditions | The Sign-In process encounters an internal error. |
| Sequence | Submit the Sign-In form, triggering an internal error. |
| Input Values | N/A |
| Expected Result | Error is logged.  Error notification is generated for further investigation. |
| Post-conditions | Error is flagged for investigation and resolution. |

**User Email Update**

Test Case 17: Successful Email Address Update

|  |  |
| --- | --- |
| Test Case ID | TC017 |
| Title | Successful Email Address Update |
| Pre-conditions | The user is logged in as “[john.doe@example.com](mailto:john.doe@example.com)” and has access to the email address update functionality. |
| Sequence | Click on the "Update" button  Enter the current password for authentication.  Enter a valid new email address.  Click on the "Duplicate Check" button.  Click on the "Generate OTP" button.  Retrieve the OTP sent to the new email address.  Enter the OTP within the specified timeframe.  Click on the "Confirm" button. |
| Input Values | Current Password: Abc123!@#  New Email Address: newemail@example.com  OTP: ValidOTP |
| Expected Result | User's email address is successfully updated to the new email address.  User receives a notification to their existing email address confirming the email address change. |
| Post-conditions | The user's email address is updated in the system and they can now log in using the new email address. |

Test Case 18: Incorrect Password

|  |  |
| --- | --- |
| Test Case ID | TC018 |
| Title | Incorrect Password |
| Pre-conditions | The user is logged in as “[john.doe@example.com](mailto:john.doe@example.com)” and has access to the email address update functionality. |
| Sequence | Click on the "Update" option.  Enter an incorrect password for authentication.  Click on the "Submit" button. |
| Input Values | Current Password: IncorrectPassword123  New Email Address: newemail@example.com |
| Expected Result | Error message displayed indicating an incorrect password. |
| Post-conditions | The user is prompted to enter the correct password for authentication. |

Test Case 19: Invalid Email Address Format

|  |  |
| --- | --- |
| Test Case ID | TC019 |
| Title | Invalid Email Address Format |
| Pre-conditions | The user is logged in as “[john.doe@example.com](mailto:john.doe@example.com)” and has access to the email address update functionality. |
| Sequence | Click on the "Update" option.  Enter the current password for authentication.  Enter an invalid email address format.  Click on the "Duplicate Check" button. |
| Input Values | Current Password: CurrentPassword123  New Email Address: invalidemail |
| Expected Result | Error message displayed indicating an invalid email address format. |
| Post-conditions | The user is prompted to enter a valid email address format. |

Test Case 20: OTP Expiry

|  |  |
| --- | --- |
| Test Case ID | TC020 |
| Title | OTP Expiry |
| Pre-conditions | The user is logged in as “[john.doe@example.com](mailto:john.doe@example.com)” and has access to the email address update functionality. |
| Sequence | Click on the "Update" button.  Enter the current password for authentication.  Enter a valid new email address.  Click on the "Generate OTP" button.  Retrieve the OTP sent to the new email address.  Wait until the OTP has expired.  Enter the expired OTP.  Click on the "Verify OTP" button. |
| Input Values | Current Password: Abc123!@#  New Email Address: newemail@example.com  OTP: ExpiredOTP |
| Expected Result | Error message displayed indicating an expired OTP. |
| Post-conditions | The user is prompted to request a new OTP. |

Test Case 21: Error Logging

|  |  |
| --- | --- |
| Test Case ID | TC021 |
| Title | Error Logging |
| Pre-conditions | The email address update process encounters an internal error. |
| Sequence | Click on the "Update" button.  Enter the current password for authentication.  Enter a valid new email address.  Click on the "Generate OTP" button, triggering an internal error. |
| Input Values | Current Password: Abc123!@#  New Email Address: newemail@example.com |
| Expected Result | Error is logged.  Error notification is generated for further investigation. |
| Post-conditions | Error is flagged for investigation and resolution. |

**Periodic Password Reset**

Test Case 22: Password Reset Prompt

|  |  |
| --- | --- |
| Test Case ID | TC022 |
| Title | Password Reset Prompt |
| Pre-conditions | The user is logged in and the password reset condition is met (exceeds 30 days since last password reset). |
| Sequence | User logs in.  System compares the current date with the user's last password reset date.  Password reset condition is met.  System prompts the user to reset their password upon next Sign-In. |
| Input Values | N/A |
| Expected Result | User sees a notification or message indicating that their password needs to be reset.  User is not allowed to access the system until they reset their password. |
| Post-conditions | User is prompted to reset their password before accessing the system. |

Test Case 23: Password Reset Notification

|  |  |
| --- | --- |
| Test Case ID | TC023 |
| Title | Password Reset Notification |
| Pre-conditions | The user is logged in and the password reset condition is not met. |
| Sequence | User logs in.  System compares the current date with the user's last password reset date.  Password reset condition is not met.  System displays a notification to the user indicating when their password is due for a reset. |
| Input Values | N/A |
| Expected Result | User sees a notification or message indicating when their password is due for a reset.  User is allowed to continue using the system without any immediate password reset requirement. |
| Post-conditions | User is notified about when their password is due for a reset. |

Test Case 24: Successful Password Reset

|  |  |
| --- | --- |
| Test Case ID | TC024 |
| Title | Successful Password Reset |
| Pre-conditions | The user has requested a password reset and successfully authenticated. |
| Sequence | User initiates the password reset process.  User enters the new password and confirms it.  User submits the new password.  System validates and confirms the new password.  System updates the user's password in the database.  System logs the date and time of the password reset.  System sends a notification email to the user confirming the password change. |
| Input Values | New Password: NewPassword123  Confirm Password: NewPassword123 |
| Expected Result | User's password is successfully updated in the system's database.  User receives a notification email confirming the password change. |
| Post-conditions | User can log in using the new password and has an updated password reset date. |

Test Case 25: Password Reset Validation Failure

|  |  |
| --- | --- |
| Test Case ID | TC025 |
| Title | Password Reset Validation Failure |
| Pre-conditions | The user has requested a password reset and entered an invalid or non-matching password. |
| Sequence | User initiates the password reset process.  User enters an invalid or non-matching new password and confirms it.  User submits the new password. |
| Input Values | New Password: InvalidPassword123  Confirm Password: InvalidPassword456 |
| Expected Result | System displays an error message indicating that the new password and confirm password do not match or do not meet the validation criteria.  User is prompted to enter a valid and matching password. |
| Post-conditions | User is prompted to enter a valid and matching password for the password reset. |

Test Case 26: Password Reset Email Confirmation

|  |  |
| --- | --- |
| Test Case ID | TC026 |
| Title | Password Reset Email Confirmation |
| Pre-conditions | The user has successfully completed the password reset process. |
| Sequence | User successfully resets their password.  System sends a notification email to the user confirming the password change. |
| Input Values | N/A |
| Expected Result | User receives a notification email confirming the password change. |
| Post-conditions | User receives an email confirming the password change. |

Test Case 27: Contact Support During Password Reset

|  |  |
| --- | --- |
| Test Case ID | TC027 |
| Title | Contact Support During Password Reset |
| Pre-conditions | The user encounters issues during the password reset process or has concerns about their password security. |
| Sequence | User encounters issues during the password reset process or has concerns about their password security.  User selects the option to contact support for assistance. |
| Input Values | N/A |
| Expected Result | System provides a means for the user to contact support. |
| Post-conditions | User receives assistance or guidance from the support team regarding the password reset process or password security concerns. |

Test Case 28: Password History Check

|  |  |
| --- | --- |
| Test Case ID | TC028 |
| Title | Password History Check |
| Pre-conditions | The user is attempting to change their password. |
| Sequence | User enters a new password that has been previously used within the specified period (e.g., the last five passwords).  User submits the new password. |
| Input Values | New Password: PreviouslyUsed123 |
| Expected Result | System detects that the new password has been used before and prevents its usage.  User receives an error message indicating that the new password cannot be reused. |
| Post-conditions | User is prompted to enter a different password that has not been used within the specified period. |

Test Case 29: Password History Check (Valid Password)

|  |  |
| --- | --- |
| Test Case ID | TC029 |
| Title | Password History Check (Valid Password) |
| Pre-conditions | The user is attempting to change their password. |
| Sequence | User enters a new password that has not been previously used within the specified period (e.g., the last five passwords).  User submits the new password. |
| Input Values | New Password: NewPassword123 |
| Expected Result | System validates the new password as it has not been used before within the specified period.  User's password is successfully updated in the system's database. |
| Post-conditions | User's password is updated in the system's database and can be used for authentication. |

**Lockout due to an incorrect password**

Test Case 30: Failed Sign-In Attempt Tracking

|  |  |
| --- | --- |
| Test Case ID | TC030 |
| Title | Failed Sign-In Attempt Tracking |
| Pre-conditions | User attempts to log in with an incorrect password. |
| Sequence | User enters an incorrect password.  User submits the Sign-In form. |
| Input Values | Email address: john@example.com  Password: IncorrectPassword123 |
| Expected Result | System increments the failed Sign-In attempt count for the user by one. |
| Post-conditions | Failed Sign-In attempt count for the user is incremented by one. |

Test Case 31: Successful Sign-In

|  |  |
| --- | --- |
| Test Case ID | TC031 |
| Title | Successful Sign-In |
| Pre-conditions | User attempts to log in with the correct password. |
| Sequence | User enters the correct password.  User submits the Sign-In form. |
| Input Values | Email address: john.doe@example.com  Password: Abc123!@# |
| Expected Result | System resets the failed Sign-In attempt count for the user to zero.  User successfully logs in. |
| Post-conditions | Failed Sign-In attempt count for the user is reset to zero, and the user is logged in. |

Test Case 32: Account Lockout

|  |  |
| --- | --- |
| Test Case ID | TC032 |
| Title | Account Lockout |
| Pre-conditions | User attempts to log in with an incorrect password exceeding the predefined threshold. |
| Sequence | User enters an incorrect password multiple times, exceeding the predefined threshold (three).  User submits the Sign-In form. |
| Input Values | Email address: john.doe@example.com  Password: IncorrectPassword123 (used three times) |
| Expected Result | System increments the failed Sign-In attempt count for the user by one for each attempt.  System detects that the failed Sign-In attempt count exceeds the predefined threshold and locks the user's account.  User receives an appropriate error message indicating that their account has been locked due to excessive failed Sign-In attempts.  System logs the account lockout event for auditing and security purposes. |
| Post-conditions | User's account is locked, and the failed Sign-In attempt count is incremented. |

Test Case 33: Account Lockout Duration

|  |  |
| --- | --- |
| Test Case ID | TC033 |
| Title | Account Lockout Duration |
| Pre-conditions | User attempts to access their locked account during the lockout duration. |
| Sequence | User enters the correct password to log in.  User submits the Sign-In form. |
| Input Values | Email address: john@example.com  Password: CorrectPassword123 |
| Expected Result | System detects that the user's account is locked and prevents access, regardless of the password entered.  User receives an appropriate error message indicating that their account is locked.  System displays a countdown timer indicating the remaining lockout duration for the user. |
| Post-conditions | User is unable to log in due to account lockout. |

Test Case 34: Account Automatic Unlock

|  |  |
| --- | --- |
| Test Case ID | TC034 |
| Title | Account Automatic Unlock |
| Pre-conditions | User's account is locked due to excessive failed Sign-In attempts. |
| Sequence | User waits for the lockout duration to elapse.  User attempts to log in with the correct password. |
| Input Values | Email address: john@example.com  Password: CorrectPassword123 |
| Expected Result | System automatically unlocks the user's account after the lockout duration has elapsed.  User is able to log in successfully. |
| Post-conditions | User's account is unlocked, and the user is logged in. |

Test Case 35: Account Lockout Email Notification

|  |  |
| --- | --- |
| Test Case ID | TC035 |
| Title | Account Lockout Email Notification |
| Pre-conditions | User's account is locked due to excessive failed Sign-In attempts. |
| Sequence | User's account reaches the threshold for failed Sign-In attempts, and the account is locked.  System sends an email notification to the user informing them of the account lockout. |
| Input Values | N/A |
| Expected Result | User receives an email notification stating that their account has been locked due to excessive failed Sign-In attempts.  Email notification includes information about the lockout duration and a link to contact support for assistance. |
| Post-conditions | User receives an email notification about the account lockout. |

Test Case 36: Password Reset during Account Lockout

|  |  |
| --- | --- |
| Test Case ID | TC036 |
| Title | Password Reset during Account Lockout |
| Pre-conditions | User's account is locked due to excessive failed Sign-In attempts. |
| Sequence | User clicks on the "Forgot Password" form  User enters their registered email address in the password recovery form.  User submits the password recovery form. |
| Input Values | Email Address: john@example.com |
| Expected Result | System verifies the user's email address and confirms that the account is currently locked.  System sends a password recovery email to the user's registered email address, providing instructions to reset the password during the account lockout period.  User receives the password recovery email with an OTP to reset their password. |
| Post-conditions | User receives a password recovery email with instructions to reset the password during the account lockout period. |

**Unique ID & Contact list**

Test Case 44: Display unique contact identifier

|  |  |
| --- | --- |
| Test Case ID | TC044 |
| Title | Display unique contact identifier |
| Pre-conditions | N/A |
| Sequence | User has successfully logs in the system. |
| Input Values | N/A |
| Expected Result | Displayed contact lists (last name, first name, e-mail, contact identifier).  No other user in the system has the same contact identifier. |
| Post-conditions | N/A |

Test Case 45: Display contact name instead of contact identifier

|  |  |
| --- | --- |
| Test Case ID | TC045 |
| Title | Display contact name instead of contact identifier |
| Pre-conditions | The contact list contains a contact with associated contact identifier. |
| Sequence | User initiates a video call with a contact. |
| Input Values | N/A |
| Expected Result | The application displays the contact's name instead of the contact identifier during the video call. |
| Post-conditions | The video call is connected with the correct contact. |

**Call**

Test Case 46: Initiate a call using a contact identifier

|  |  |
| --- | --- |
| Test Case ID | TC046 |
| Title | Initiate a call using a contact identifier |
| Pre-conditions | User is logged in and has access to the contact identifier. |
| Sequence | User enters a valid contact identifier to initiate a call. |
| Input Values | Contact identifier (valid) |
| Expected Result | The call is successfully initiated with the specified contact.  The call log is updated with the call start time, duration, participants, and call outcome. |
| Post-conditions | The call log is updated with the call details. |

Test Case 47: View call history

|  |  |
| --- | --- |
| Test Case ID | TC047 |
| Title | View call history |
| Pre-conditions | User has made previous calls and the call history is available. |
| Sequence | User navigates to the call history feature. |
| Input Values | N/A |
| Expected Result | The call history is displayed, showing past calls with details like participants, timestamps, and call duration. |
| Post-conditions | The call history is displayed to the user. |

Test Case 48: Check call status and outcome during call initiation

|  |  |
| --- | --- |
| Test Case ID | TC048 |
| Title | Check call status and outcome during call initiation |
| Pre-conditions | User is initiating a call. |
| Sequence | User initiates a call. |
| Input Values | N/A |
| Expected Result | The user is presented with the call status (e.g., ringing) during call initiation.  The call outcome is displayed once the call is answered, busy, or rejected. |
| Post-conditions | The user is informed about the call status and outcome. |

Test Case 49: End the call during call initiation

|  |  |
| --- | --- |
| Test Case ID | TC049 |
| Title | End the call during call initiation |
| Pre-conditions | User is initiating a call. |
| Sequence | User initiates a call.  User chooses to end the call. |
| Input Values | N/A |
| Expected Result | The call initiation process is interrupted, and the call is not connected. |
| Post-conditions | The call initiation process is terminated. |

**Connection, Notice and Disconnect**

Test Case 50: Accept incoming call

|  |  |
| --- | --- |
| Test Case ID | TC050 |
| Title | Accept incoming call |
| Pre-conditions | User is logged in and is not currently in a call. |
| Sequence | User receives an incoming call notification.  User selects the option to accept the call. |
| Input Values | Selected option = Accept |
| Expected Result | The system establishes the call connection.  The user interface transitions to the active call screen, showing the contact name of the caller. |
| Post-conditions | The user is in an active call with the caller. |

Test Case 51: Reject incoming call

|  |  |
| --- | --- |
| Test Case ID | TC051 |
| Title | Reject incoming call |
| Pre-conditions | User is logged in and is not currently in a call. |
| Sequence | User receives an incoming call notification.  User selects the option to reject the call. |
| Input Values | Selected option = Reject |
| Expected Result | The incoming call is terminated.  The user interface remains in the current state. |
| Post-conditions | The user is not in a call and returns to their previous state. |

Test Case 52: Missed call notification (call not accepted)

|  |  |
| --- | --- |
| Test Case ID | TC052 |
| Title | Missed call notification (call not accepted) |
| Pre-conditions | User is logged in and has missed an incoming call. |
| Sequence | User receives a missed call notification.  User opens the missed call notification. |
| Input Values | N/A |
| Expected Result | The system displays the missed call information, including the contact identifier or contact name of the caller. |
| Post-conditions | The user is informed about the missed call. |

Test Case 53: Missed call notification (called entity in another call)

|  |  |
| --- | --- |
| Test Case ID | TC053 |
| Title | Missed call notification (called entity in another call) |
| Pre-conditions | User is logged in and has missed an incoming call due to the called entity being in another call. |
| Sequence | User receives a missed call notification.  User opens the missed call notification. |
| Input Values | N/A |
| Expected Result | The system displays the missed call information, including the contact identifier or contact name of the caller. |
| Post-conditions | The user is informed about the missed call. |

Test Case 54: Call termination notification

|  |  |
| --- | --- |
| Test Case ID | TC054 |
| Title | Call termination notification |
| Pre-conditions | User A and User B are engaged in an active call. |
| Sequence | User A terminates the call. |
| Input Values | Termination action by User A |
| Expected Result | User B receives a call termination notification. |
| Post-conditions | The call is ended for both User A and User B. |

Test Case 55: Application brought to the foreground during incoming call

|  |  |
| --- | --- |
| Test Case ID | TC055 |
| Title | Application brought to the foreground during incoming call |
| Pre-conditions | User is logged in and the application is running in the background. |
| Sequence | User receives an incoming call. |
| Input Values | Incoming call notification |
| Expected Result | The application is brought to the foreground, becoming the active window.  The user interface displays the incoming call screen with the contact name of the caller. |
| Post-conditions | The user is presented with the incoming call screen. |

**Communication methods**

Test Case 56: Point-to-point communication functionality

|  |  |
| --- | --- |
| Test Case ID | TC056 |
| Title | Point-to-point communication functionality |
| Pre-conditions | The application is installed and running on both endpoints of the call. |
| Sequence | User A initiates a call to User B. |
| Input Values | Call initiation by User A |
| Expected Result | User B functions as the server, waiting for a response from User A.  User A functions as the client, receiving the call initiation request. |
| Post-conditions | User A and User B establish a point-to-point communication connection. |

Test Case 57: Call initiation failure

|  |  |
| --- | --- |
| Test Case ID | TC057 |
| Title | Call initiation failure |
| Pre-conditions | The application is installed and running on both endpoints of the call. |
| Sequence | User A initiates a call to User B.  User B's device is turned off or not connected to the network. |
| Input Values | Call initiation by User A |
| Expected Result | User A's application displays an error message indicating the call initiation failure.  User B's application does not receive the call initiation request. |
| Post-conditions | The call is not established due to the unavailability of User B. |

# Threat analysis

* DFD and STRIDE methodology were used to perform Threat Analysis

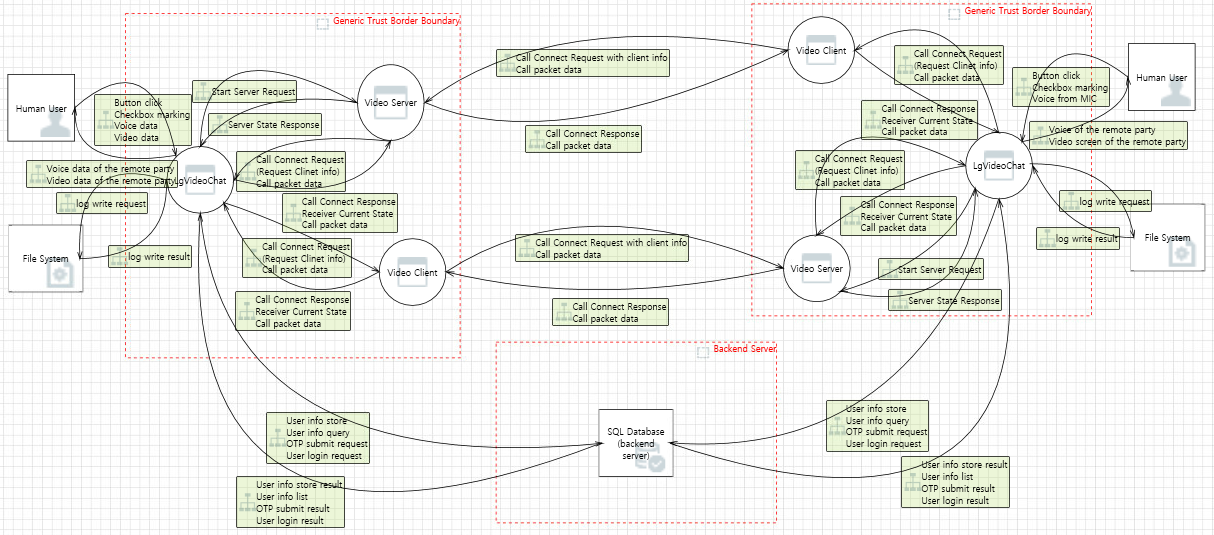




Figure . Number of Identified threats : 45

Table . Identified threat result

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| threat Id | Title | Category | Flow | Priority | Description | Identified threat, derived requirement and Mitigation | Deisgn or solution proposal |
| 15 | Spoofing the LgVideoChat Process | Spoofing | LgVideoChat->SQL Database | 10 | LgVideoChat may be spoofed by an attacker and this may lead to unauthorized access to SQL Database (backend server). Consider using a standard authentication mechanism to identify the source process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS will be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 16 | Spoofing of Destination Data Store SQL Database (backend server) | Spoofing | LgVideoChat->SQL Database | 10 | SQL Database (backend server) may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database (backend server). Consider using a standard authentication mechanism to identify the destination data store. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 17 | Potential SQL Injection Vulnerability for SQL Database (backend server) | Tampering | LgVideoChat->SQL Database | 8 | SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker. | [Identified threat]  To execute unintended command in backend server, SQL injection attack can be performed by attacker.  This will lead to disclosure of confidential information in backend server and make attacker to use shell command.  [Security requirement]  Input validation should be performed for the data over external network.  [Mitigation]  SQL commands from external interface will be executed only when it passes internal validation fuction. | Backend server shall perform input validation. |
| 18 | The SQL Database (backend server) Data Store Could Be Corrupted | Tampering | LgVideoChat->SQL Database | 10 | Data flowing across User info store User info query OTP submit request User login request may be tampered with by an attacker. This may lead to corruption of SQL Database (backend server). Ensure the integrity of the data flow to the data store. | [Identified threat]  Attacker can corrupt the data in the middle of the network.  It will lead to store wrong information in backend server or send wrong request to backend server.  [Security requirement]  Integrity of data which is delivered over external network shall be checked.  [Mitigation]  Integrity check for all packet data. | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 19 | Data Store Denies SQL Database (backend server) Potentially Writing Data | Repudiation | LgVideoChat->SQL Database | 6 | SQL Database (backend server) claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Identified threat]  Backend server claims that it didn't receive any request from the other party.  This will make to use unnecessary resources.  [Security requirement]  Each service shall record the information which is sent or received over network.  [Mitigation]  Each service shall store log message. | Backend server shall store the log message as a file. |
| 20 | Data Flow Sniffing | Information Disclosure | LgVideoChat->SQL Database | 10 | Data flowing across User info store User info query OTP submit request User login request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Identified threat]  Data over external network can be sniffed by attacker.  It will lead to disclosure of confidential information.  [Security requirement]  Data over external network shall be encrypted.  [Mitigation]  Encryption key shall be shared between the entities which will communicate with and the data shall be encrypted using the shared key. | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 21 | Potential Excessive Resource Consumption for LgVideoChat or SQL Database (backend server) | Denial Of Service | LgVideoChat->SQL Database | 8 | Does LgVideoChat or SQL Database (backend server) take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. Only allowed APIs shall be processed in backend server. |
| 22 | Data Flow User info store User info query OTP submit request User login request Is Potentially Interrupted | Denial Of Service | LgVideoChat->SQL Database | 8 | An external agent interrupts data flowing across a trust boundary in either direction. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. Only allowed APIs shall be processed in backend server. |
| 23 | Data Store Inaccessible | Denial Of Service | LgVideoChat->SQL Database | 10 | An external agent prevents access to a data store on the other side of the trust boundary. | [Identified threat]  Data over external network can be sniffed by attacker.  It will lead to disclosure of confidential information.  [Security requirement]  Data over external network shall be encrypted.  [Mitigation]  Encryption key shall be shared between the entities which will communicate with and the data shall be encrypted using the shared key. | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 52 | Elevation by Changing the Execution Flow in LgVideoChat | Elevation Of Privilege | SQL Database->LgVideoChat | 6 | An attacker may pass data into LgVideoChat in order to change the flow of program execution within LgVideoChat to the attacker's choosing. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 51 | LgVideoChat May be Subject to Elevation of Privilege Using Remote Code Execution | Elevation Of Privilege | SQL Database->LgVideoChat | 6 | SQL Database (backend server) may be able to remotely execute code for LgVideoChat. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 50 | Data Store Inaccessible | Denial Of Service | SQL Database->LgVideoChat | 8 | An external agent prevents access to a data store on the other side of the trust boundary. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. Only allowed APIs shall be processed in LgVideoChat. |
| 49 | Data Flow User info store result User info list OTP submit result User login result Is Potentially Interrupted | Denial Of Service | SQL Database->LgVideoChat | 8 | An external agent interrupts data flowing across a trust boundary in either direction. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. Only allowed APIs shall be processed in LgVideoChat. |
| 48 | Potential Process Crash or Stop for LgVideoChat | Denial Of Service | SQL Database->LgVideoChat | 6 | LgVideoChat crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. |
| 47 | Weak Access Control for a Resource | Information Disclosure | SQL Database->LgVideoChat | 6 | Improper data protection of SQL Database (backend server) can allow an attacker to read information not intended for disclosure. Review authorization settings. | [Identified threat]  Attacker can read information using weak access control.  [Security requirement]  All data shall be protected against unauthorized access.  [Mitigation]  Permission needs to be managed through access control. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. |
| 46 | Potential Data Repudiation by LgVideoChat | Repudiation | SQL Database->LgVideoChat | 6 | LgVideoChat claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Identified threat]  LgVideoChat claims that it didn't receive any request from the other party.  This will make to use unnecessary resources.  [Security requirement]  Each service shall record the information which is sent or received over network.  [Mitigation]  Each service shall store log message. | LgVideoChat shall store the log message as a file. |
| 45 | Spoofing of Source Data Store SQL Database (backend server) | Spoofing | SQL Database->LgVideoChat | 10 | SQL Database (backend server) may be spoofed by an attacker and this may lead to incorrect data delivered to LgVideoChat. Consider using a standard authentication mechanism to identify the source data store. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 44 | Spoofing the LgVideoChat Process | Spoofing | SQL Database->LgVideoChat | 10 | LgVideoChat may be spoofed by an attacker and this may lead to information disclosure by SQL Database (backend server). Consider using a standard authentication mechanism to identify the destination process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 70 | Spoofing the Video Server Process | Spoofing | Video Server->Video Client | 10 | Video Server may be spoofed by an attacker and this may lead to unauthorized access to Video Client. Consider using a standard authentication mechanism to identify the source process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack.  2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied  CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between LgVideoChat and Backend server.  For the detailed design, please refer to detailed design document. |
| 71 | Spoofing the Video Client Process | Spoofing | Video Server->Video Client | 10 | Video Client may be spoofed by an attacker and this may lead to information disclosure by Video Server. Consider using a standard authentication mechanism to identify the destination process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack.  2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied  CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 72 | Potential Lack of Input Validation for Video Client | Tampering | Video Server->Video Client | 10 | Data flowing across Call Connect Response Call packet data may be tampered with by an attacker. This may lead to a denial of service attack against Video Client or an elevation of privilege attack against Video Client or an information disclosure by Video Client. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Identified threat]  Attacker can corrupt the data in the middle of the network.  It will lead to store wrong information or send wrong request to the other party.  [Security requirement]  Integrity of data which is delivered over external network shall be checked.  [Mitigation]  Integrity check for all packet data. | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 73 | Potential Data Repudiation by Video Client | Repudiation | Video Server->Video Client | 6 | Video Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Identified threat]  Application claims that it didn't receive any request from the other party.  This will make to use unnecessary resources.  [Security requirement]  Each service shall record the information which is sent or received over network.  [Mitigation]  Each service shall store log message. | LgVideoChat shall store the log message as a file. |
| 74 | Data Flow Sniffing | Information Disclosure | Video Server->Video Client | 10 | Data flowing across Call Connect Response Call packet data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Identified threat]  Data over external network can be sniffed by attacker.  It will lead to disclosure of confidential information.  [Security requirement]  Data over external network shall be encrypted.  [Mitigation]  Encryption key shall be shared between the entities which will communicate with and the data shall be encrypted using the shared key. | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 75 | Potential Process Crash or Stop for Video Client | Denial Of Service | Video Server->Video Client | 6 | Video Client crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between Video Server and Video Client. DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. |
| 76 | Data Flow Call Connect Response Call packet data Is Potentially Interrupted | Denial Of Service | Video Server->Video Client | 6 | An external agent interrupts data flowing across a trust boundary in either direction. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between Video Server and Video Client. DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. |
| 77 | Elevation Using Impersonation | Elevation Of Privilege | Video Server->Video Client | 6 | Video Client may be able to impersonate the context of Video Server in order to gain additional privilege. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 78 | Video Client May be Subject to Elevation of Privilege Using Remote Code Execution | Elevation Of Privilege | Video Server->Video Client | 6 | Video Server may be able to remotely execute code for Video Client. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 79 | Elevation by Changing the Execution Flow in Video Client | Elevation Of Privilege | Video Server->Video Client | 6 | An attacker may pass data into Video Client in order to change the flow of program execution within Video Client to the attacker's choosing. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 102 | Spoofing the Video Client Process | Spoofing | Video Client->Video Server | 10 | Video Client may be spoofed by an attacker and this may lead to unauthorized access to Video Server. Consider using a standard authentication mechanism to identify the source process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 103 | Spoofing the Video Server Process | Spoofing | Video Client->Video Server | 10 | Video Server may be spoofed by an attacker and this may lead to information disclosure by Video Client. Consider using a standard authentication mechanism to identify the destination process. | [Identified threat]  1. The attacker disguises his identity by changing the Mac Address through an ARP spoofing attack. 2. The attacker intercepts and corrupts the information transmitted to the other party through the MITM attack.  [Security requirement]  There must be a standard authentication mechanism for source process identification.  [Mitigation]  PKI-based server/client authentication must be applied CA certificate and server certificate for LgVideoChat must be issued | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 104 | Potential Lack of Input Validation for Video Server | Tampering | Video Client->Video Server | 10 | Data flowing across Call Connect Request with client info Call packet data may be tampered with by an attacker. This may lead to a denial of service attack against Video Server or an elevation of privilege attack against Video Server or an information disclosure by Video Server. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Identified threat]  Attacker can corrupt the data in the middle of the network.  It will lead to store wrong information or send wrong request to the other party.  [Security requirement]  Integrity of data which is delivered over external network shall be checked.  [Mitigation]  Integrity check for all packet data. | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 105 | Potential Data Repudiation by Video Server | Repudiation | Video Client->Video Server | 6 | Video Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Identified threat]  Application claims that it didn't receive any request from the other party.  This will make to use unnecessary resources.  [Security requirement]  Each service shall record the information which is sent or received over network.  [Mitigation]  Each service shall store log message. | LgVideoChat shall store the log message as a file. |
| 106 | Data Flow Sniffing | Information Disclosure | Video Client->Video Server | 10 | Data flowing across Call Connect Request with client info Call packet data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Identified threat]  Data over external network can be sniffed by attacker.  It will lead to disclosure of confidential information.  [Security requirement]  Data over external network shall be encrypted.  [Mitigation]  Encryption key shall be shared between the entities which will communicate with and the data shall be encrypted using the shared key. | TLS shall be applied to the communication between Video Server and Video Client.  For the detailed design, please refer to detailed design document. |
| 107 | Potential Process Crash or Stop for Video Server | Denial Of Service | Video Client->Video Server | 8 | Video Server crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between LgVideoChat and Backend server. Only allowed APIs shall be processed in LgVideoChat. |
| 108 | Data Flow Call Connect Request with client info Call packet data Is Potentially Interrupted | Denial Of Service | Video Client->Video Server | 6 | An external agent interrupts data flowing across a trust boundary in either direction. | [Identified threat]  Attacker can send excessive packet to the application or backend server.  This will lead to denial of service of each entity.  [Security requirement]  Each service shall be available all the time.  [Mitigation]  Mutual authentication shall be performed before starting communication.  Permission needs to be managed through access control. | TLS shall be applied to the communication between Video Server and Video Client. DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. |
| 109 | Elevation Using Impersonation | Elevation Of Privilege | Video Client->Video Server | 6 | Video Server may be able to impersonate the context of Video Client in order to gain additional privilege. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 110 | Video Server May be Subject to Elevation of Privilege Using Remote Code Execution | Elevation Of Privilege | Video Client->Video Server | 6 | Video Client may be able to remotely execute code for Video Server. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 111 | Elevation by Changing the Execution Flow in Video Server | Elevation Of Privilege | Video Client->Video Server | 6 | An attacker may pass data into Video Server in order to change the flow of program execution within Video Server to the attacker's choosing. | [Identified threat]  Attacker can send shell code and it will have excessive permission.  [Security requirement]  For each user, least privileage shall be applied.  Input validation should be performed for the data over external network.  [Mitigation]  Each user shall have least privileage.  All input data from external network will be checked by internal validation fuction. | DAC policy shall be applied properly for LgVideoChat. Admin or root permission shall not be allowed for LgVideoChat. LgVideoChat shall validate input data which is delivered for video call. |
| 116 | Spoofing of Destination Data Store File System | Spoofing | LgVideoChat->File System | 4 | File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store. | [Identified threat]  Attacker can replace the file system with the one of attacker's.  It will lead to store the log information to attacker's storage.  [Security requirement]  File system shall have protection method against replacing it.  [Mitigation]  Hard disk drive shall be sealed with a sticker so that it can be detected when replacing is occurred. | Sealing sticker shall be applied to the laptop which has LgVideoChat application |
| 119 | Weak Access Control for a Resource | Information Disclosure | LgVideoChat->File System | 4 | Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings. | [Identified threat]  Attacker can read log message from file system and it can lead to disclosure of confidential information.  [Security requirement]  Log message shall be encrypted.  [Mitigation]  Log message shall be encrypted and stored to file system. | LgVideoChat shall encrypt log file. |
| 201 | Spoofing of the Human User External Destination Entity | Spoofing | LgVideoChat->Human User | 10 | Human User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Human User. Consider using a standard authentication mechanism to identify the external entity. | [Identified threat]  An attacker can issue malicious commands through identity disguise, causing unintended actions by the user.  [Security requirement]  Require enhanced authentication for user login  [Mitigation]  Two factor authentication based on password and otp should be applied. | Two factor authentication shall be applied to login to the LgVideoChat with following method. 1. password 2. OTP number using private email address  For the detailed design, please refer to detailed design document. |
| 199 | Elevation by Changing the Execution Flow in LgVideoChat | Elevation Of Privilege | Human User->LgVideoChat | 10 | An attacker may pass data into LgVideoChat in order to change the flow of program execution within LgVideoChat to the attacker's choosing. | [Identified threat]  An attacker can issue malicious commands through identity disguise, causing unintended actions by the user.  [Security requirement]  Require enhanced authentication for user login  [Mitigation]  Two factor authentication based on password and otp should be applied. | Two factor authentication shall be applied to login to the LgVideoChat with following method. 1. password 2. OTP number using private email address  For the detailed design, please refer to detailed design document. |
| 198 | LgVideoChat May be Subject to Elevation of Privilege Using Remote Code Execution | Elevation Of Privilege | Human User->LgVideoChat | 10 | Human User may be able to remotely execute code for LgVideoChat. | [Identified threat]  An attacker can issue malicious commands through identity disguise, causing unintended actions by the user.  [Security requirement]  Require enhanced authentication for user login  [Mitigation]  Two factor authentication based on password and otp should be applied. | Two factor authentication shall be applied to login to the LgVideoChat with following method. 1. password 2. OTP number using private email address  For the detailed design, please refer to detailed design document. |
| 197 | Elevation Using Impersonation | Elevation Of Privilege | Human User->LgVideoChat | 10 | LgVideoChat may be able to impersonate the context of Human User in order to gain additional privilege. | [Identified threat]  An attacker can issue malicious commands through identity disguise, causing unintended actions by the user.  [Security requirement]  Require enhanced authentication for user login  [Mitigation]  Two factor authentication based on password and otp should be applied. | Two factor authentication shall be applied to login to the LgVideoChat with following method. 1. password 2. OTP number using private email address  For the detailed design, please refer to detailed design document. |
| 191 | Spoofing the Human User External Entity | Spoofing | Human User->LgVideoChat | 10 | Human User may be spoofed by an attacker and this may lead to unauthorized access to LgVideoChat. Consider using a standard authentication mechanism to identify the external entity. | [Identified threat]  An attacker can issue malicious commands through identity disguise, causing unintended actions by the user.  [Security requirement]  Require enhanced authentication for user login  [Mitigation]  Two factor authentication based on password and otp should be applied. | Two factor authentication shall be applied to login to the LgVideoChat with following method. 1. password 2. OTP number using private email address  For the detailed design, please refer to detailed design document. |

# Security requirements & Mitigation

* Prioritized each threat through team workshop
* Resulted in various score : 4, 6, 8, 10
* **Key Security Requirements & Mitigations** from high priority threats (Score 6, 8, 10) are as follows

|  |
| --- |
| Security requirements & Mitigations |
| **PKI-based server authentication for App and Backend Server** |
| **Secure communication between Apps** |
| **Secure communication between App and Backend Server** |
| **Two factor authentication using password and OTP to email** => Initial requirement has been specified in detail |
| **Input validation check by Backend Server** |
| **Storing log file by App and Backend server** |

# System design

## Initial Design

Initial system architecture from given requirements was designed as follows

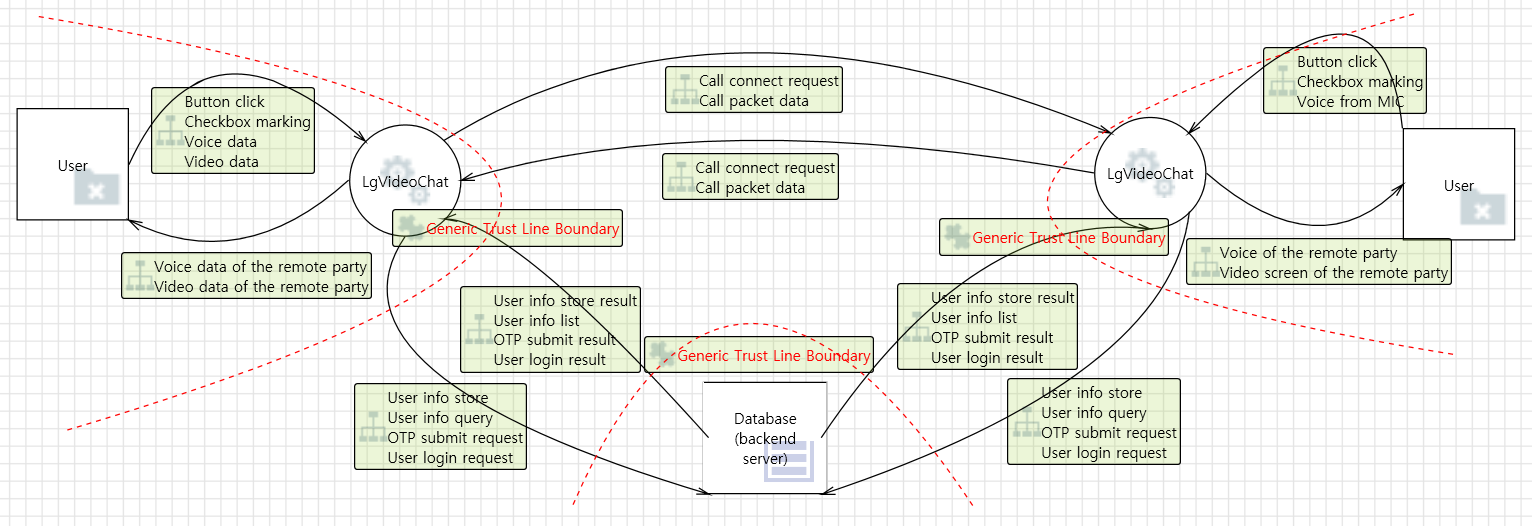


Figure . Initial Design reflecting all system entities and communication data

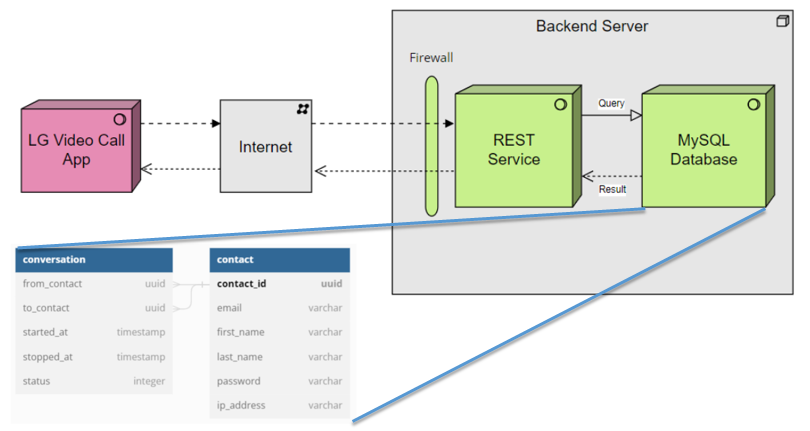


Figure . Initial Design for backend server

## Design Improvement including Mitigation

After completing threat analysis, system design was improved by security requirements and mitigations

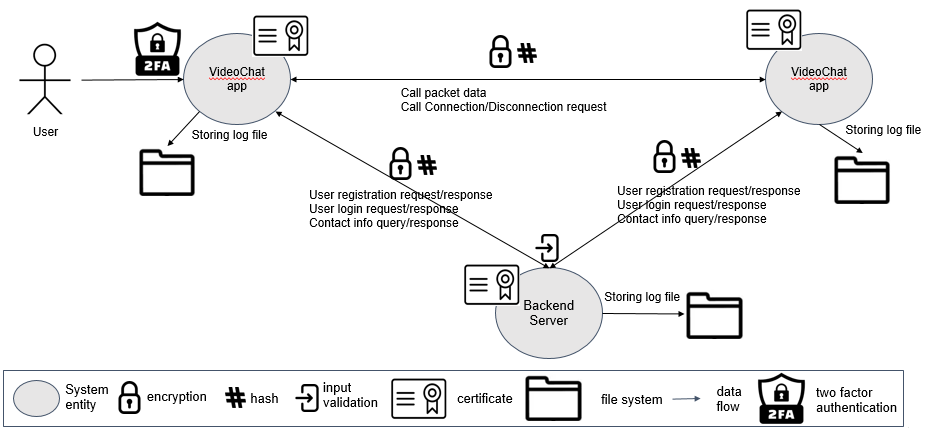


Figure . Overall system design

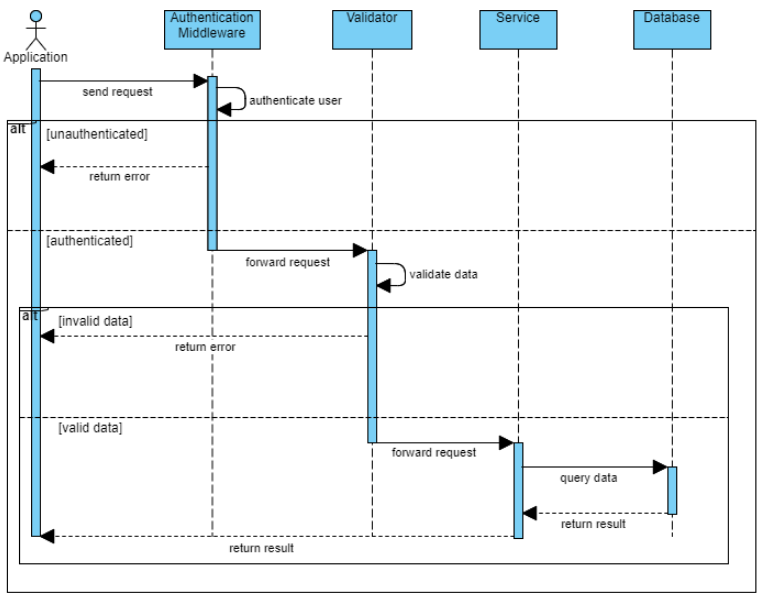


Figure . Input Validation Check by Backend Server

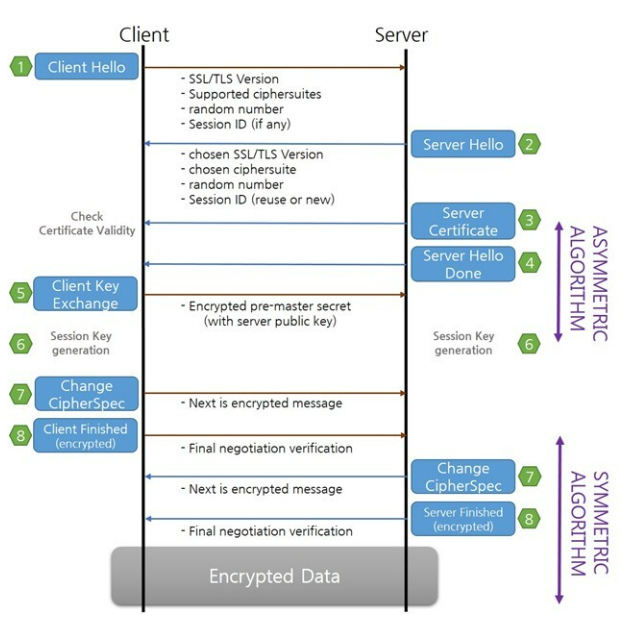


Figure . Secure Communication & authentication

* PKI-based server authentication for both Application and Backend Server
* Secure communication between Applications
* Secure communication between Application and Backend Server
* **Adopted Solution : TLS v1.3**

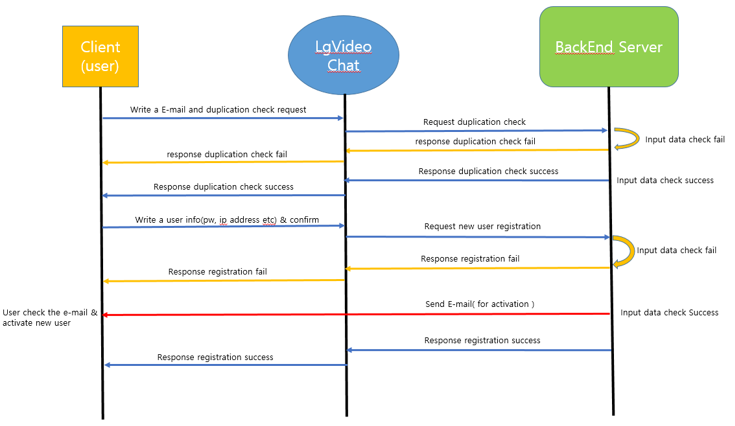


Figure . Two factor authentication (User registration)

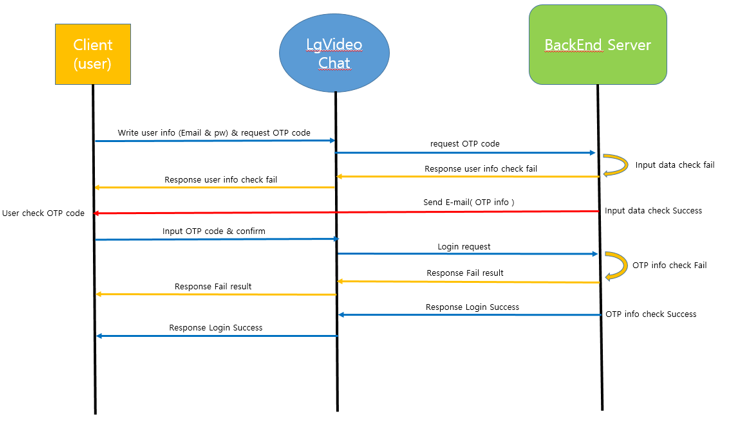


Figure . Two factor authentication (User login)

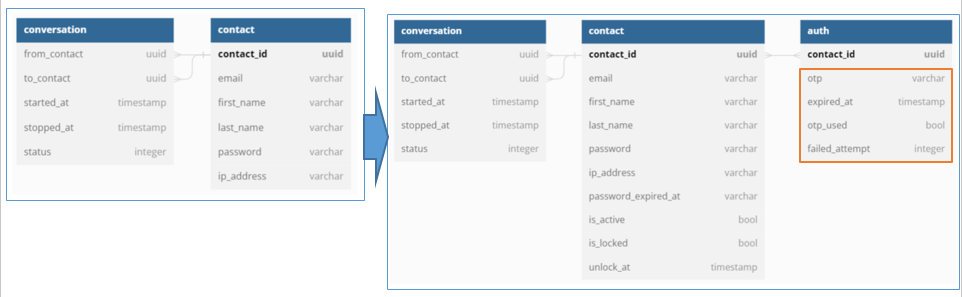


Figure . database table design for two factor authentication

## Backend Server API design

To support security requirements, APIs provided by backend server are defined as follows.

**Sign Up**

# Signup example

$ curl -k https://20.119.70.194/api/user/signup -X POST -d "email=viet.truong@lge.com&password=TestP4ss!@#&confirm\_password=TestP4ss!@#&ip\_address=192.168.11.11&first\_name=Viet&last\_name=Truong"

{"message":"User created successfully. Please check your email to activate your account!"}

# Open https://ethereal.email/mesages (login with chaim48@ethereal.email / eezpJY5ZAR8V9hRQbT), open the email and click on the link to activate the account

Go to Ethereal email and click to the activation link to activate your account.

**Login**

$ curl -k https://20.119.70.194/api/user/generate-otp?email=viet.truong.tae@lge.com

{"message":"OTP has been sent to the email"}

# Send request to verify OTP

$ curl.exe -k https://20.119.70.194/api/auth/login -X POST -d "email=viet.truong@lge.com&password=TestP4ss!@#&otp=123456"

{"message":"Successfully login","access\_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiMGU2MmIzYjUtMGFjZi0xMWVlLTlkYmUtNjA0NWJkZGM5NGY3IiwiaWF0IjoxNjg2NzU5NjAzLCJleHAiOjE2ODY4NDYwMDN9.u-rMAHspFsu6LUL6Bb-2HXmma\_foYowSNQsO3BNkxso"}

**Authorization Header**

# Use access token to authenticate.

$ curl -k https://20.119.70.194/api/users -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiMGU2MmIzYjUtMGFjZi0xMWVlLTlkYmUtNjA0NWJkZGM5NGY3IiwiaWF0IjoxNjg2NzU5NjAzLCJleHAiOjE2ODY4NDYwMDN9.u-rMAHspFsu6LUL6Bb-2HXmma\_foYowSNQsO3BNkxso"

# each page contains 10 users

$ curl -k https://20.119.70.194/api/users?page=2 -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiMGU2MmIzYjUtMGFjZi0xMWVlLTlkYmUtNjA0NWJkZGM5NGY3IiwiaWF0IjoxNjg2NzU5NjAzLCJleHAiOjE2ODY4NDYwMDN9.u-rMAHspFsu6LUL6Bb-2HXmma\_foYowSNQsO3BNkxso"

{"data":[],"meta":{"page":2}}

**Check Email**

$ curl -k https://20.119.70.194/api/user/check-email -X POST -d "email=viet.truong@lge.com"

Status code: 403 Forbidden

{"message":"Email existed"}

$ curl -k https://20.119.70.194/api/user/check-email -X POST -d "email=viet2.truong@lge.com"

Status code: 200 OK

{"message":"Email does not exist"}

**Query User Information From IP Address**

$ curl -k https://localhost/api/user/get-info-from-ip -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d "ip\_address=192.168.1.2"

Status code: 200 OK

{"contact\_id":"69b72431-0e51-11ee-8925-080027030fc4","email":"quangviet911@gmail.com","first\_name":"Viet","last\_name":"Quang","ip\_address":"192.168.1.2"}

$ curl -k https://localhost/api/user/get-info-from-ip -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d "ip\_address=192.168.1.23"

Status code: 400 Bad Request

{"message":"Unable to find user with this IP address"}

**Get User Information**

$ curl -k https://localhost/api/user/me -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MTg0MDYxLCJleHAiOjE2ODcyNzA0NjF9.ZrHFDX7Nc8C6p9gNMOobkFUKLOywB4CuMpSzveUtcXU"

{"contact\_id":"69b72431-0e51-11ee-8925-080027030fc4","email":"quangviet910@gmail.com","last\_name":"Quang","first\_name":"Viet","ip\_address":"192.168.1.2","password":"$2b$06$R6vakM65xf4Oh2y68yro0uJa.6JqIhdPKOJwIZ.H4Sac3shCSI4Ki"}

**Get Information of All Registered Users**

$ curl -k https://20.119.70.194/api/user/all -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiN2MxOWI2ZTMtMTA1Mi0xMWVlLTlkYmUtNjA0NWJkZGM5NGY3IiwiaWF0IjoxNjg3NDEwNDkxLCJleHAiOjE2ODc0OTY4OTF9.y6Y5tiDiz43mEK3wTSCTD1cP6tK8feDzfp-vGeUvbGo"

{"data":[{"contact\_id":"054b8da6-10b8-11ee-9dbe-6045bddc94f7","email":"hongjae1.lim@lge.com","last\_name":"Lim","first\_name":"Hongjae","ip\_address":"192.168.0.126"},{"contact\_id":"69474282-10ac-11ee-9dbe-6045bddc94f7","email":"john.doe@example.com","last\_name":"doe","first\_name":"john","ip\_address":"192.168.0.212"},{"contact\_id":"040fa4c4-108d-11ee-9dbe-6045bddc94f7","email":"minji.tae@lge.com","last\_name":"Tae","first\_name":"Minji","ip\_address":"127.0.0.5"},{"contact\_id":"5618a336-10b8-11ee-9dbe-6045bddc94f7","email":"quangviet910@gmail.com","last\_name":"Vo","first\_name":"Hau","ip\_address":"127.0.0.2"},{"contact\_id":"8a77e852-10ac-11ee-9dbe-6045bddc94f7","email":"sch830414.test@gmail.com","last\_name":"sung","first\_name":"chanhun","ip\_address":"10.177.249.171"},{"contact\_id":"5a9291db-10b8-11ee-9dbe-6045bddc94f7","email":"test1@example.com","last\_name":"2","first\_name":"1","ip\_address":"192.168.1.212"},{"contact\_id":"be596a89-10b9-11ee-9dbe-6045bddc94f7","email":"test2@example.com","last\_name":"2","first\_name":"1","ip\_address":"192.168.1.2"},{"contact\_id":"7c19b6e3-1052-11ee-9dbe-6045bddc94f7","email":"viet.truong@lge.com","last\_name":"Truong","first\_name":"Viet","ip\_address":"127.0.0.1"}],"meta":{"page":1}}

**Generate OTP**

$ curl -k https://localhost/api/user/generate-otp -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MTg0MDYxLCJleHAiOjE2ODcyNzA0NjF9.ZrHFDX7Nc8C6p9gNMOobkFUKLOywB4CuMpSzveUtcXU"

Status code: 200 OK

{"message":"OTP is sent to the new email"}

**Update Email Only**

$ curl -k https://localhost/api/user/update -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d 'current\_password=TestP4ss!@#&new\_email=quangviet911@gmail.com&otp=630573'

Status code: 400 Bad Request

{"message":"Invalid OTP"}

$ curl -k https://localhost/api/user/update -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d 'current\_password=TestP4ss!@#&new\_email=quangviet911@gmail.com&otp=612345'

Status code: 200 OK

{"message":"User data updated"}

**Update Password Only**

$ curl -k https://localhost/api/user/update -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d 'current\_password=Qviet1997!@#&new\_password=Qviet1997!@#&confirm\_new\_password=Qviet1997!@#&otp=630573'

Status code: 200 OK

{"message":"Updated user data"}

**Update Password & Email**

$ curl -k https://localhost/api/user/update -X POST -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiNjliNzI0MzEtMGU1MS0xMWVlLTg5MjUtMDgwMDI3MDMwZmM0IiwiaWF0IjoxNjg3MjQzODA1LCJleHAiOjE2ODczMzAyMDV9.ooFqYc2whNSn62lvFXR3Xa8OFkPIRceKHhPGWtFgJOg" -d 'current\_password=Qviet1997!@#&new\_password=Qviet1997!@#&confirm\_new\_password=Qviet1997!@#&new\_email=quangviet911@gmail.com&otp=630573'

Status code: 200 OK

{"message":"Updated user data"}

Status code: 422 -> invalid data (example: passwords do not match)

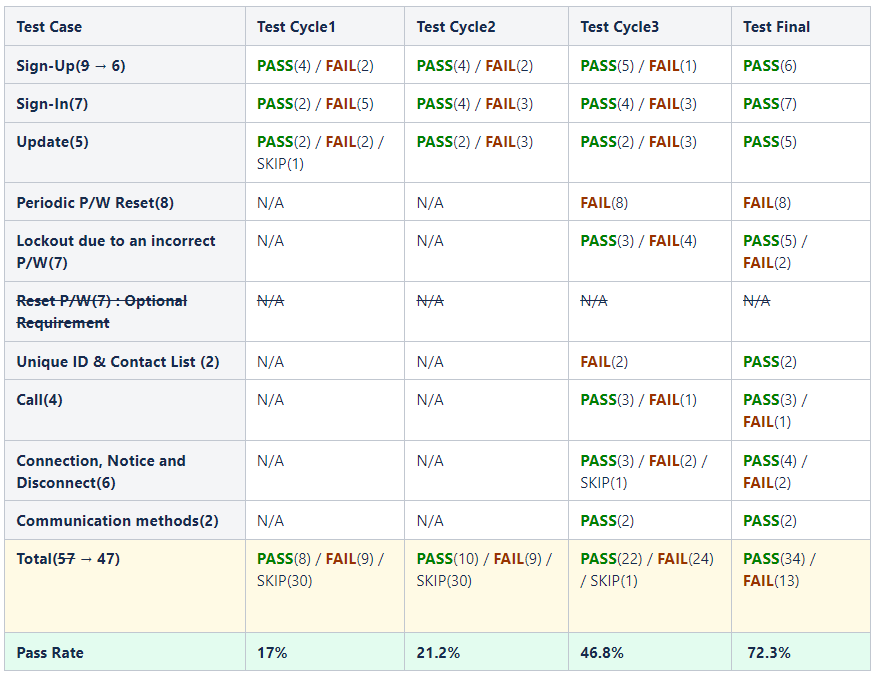
# Implementation

* **Agile methodology was applied. The reason and how …**- Started implementation before completing all design due to lack of time  
  - Need to reflect changed and added system design after threat analysis  
  - Development and Verification was performed in parallel to find bugs earlier  
  - Sync up meeting and sharing obstacles every day  
   (http://collab.lge.com/main/display/SCSPECIALT/0.+Meeting+Minute)
* **Development environment and tools**- Visual Studio Community, Beyond compare  
  - MySQL, Ethereal for Fake Email Service  
  - Self signed certificate for server authentication  
  - GitHub for sharing and integrating source code  
  - Additional library : Openssl, Boost, Nlohmann-json for application

# Verification

## Verification Overview

* Test case  
  Generated based on Functional requirements
* Test purpose  
  - To verify initial functional requirements  
  - To verify additional security requirements
* Test constraints  
  - Use Ethereal site for Fake email service  
  - Laptops testing the application should be connected through router   
  - Firewall configuration in Laptop should be disabled
* Final test result  
  - Total test cases : 47  
  - Pass : 34, Fail : 13 (not critical issues)  
  - Pass rate : 72.3%



## Verification Result Detail

* **Sign-Up**

PASS TC001 Successful Registration

PASS TC002 Invalid Email Address

PASS TC003 Existing Email Address

PASS TC004 Weak Password

PASS TC005 Password Mismatch

PASS TC008 error Logging

* **Sign-In**

PASS TC010 Successful Sign-In

PASS TC011 Invalid Email Address

PASS TC012 Incorrect Password

PASS TC013 Request OTP

PASS TC014 Invalid OTP

PASS TC015 - Successful OTP Verification

PASS TC016 - Error Logging

* **User Email Update**

PASS TC017 Successful Email Address Update

PASS TC018 Incorrect Password

PASS TC019 Invalid Email Address Format

PASS TC020 OTP Expiry

PASS TC021 Error Logging

* **Periodic Password Reset**

Not implemented yet. TC022~TC029

* **Lockout due to an incorrect password**

PASS TC030 Failed Sign-In Attempt Tracking

PASS TC031 Successful Sign-In

PASS TC032 Account Lockout

PASS TC033 Account Lockout Duration

PASS TC034 Account Automatic Unlock

PASS TC035 Account Lockout Email Notification

**FAIL** TC036 Password Reset during Account Lockout

If it is a lockout, you must provide a password reset function.

* **Unique ID & Contact list**

PASS TC044 Display unique contact identifier

PASS TC045 Display contact name instead of contact identifier

* **Call**

PASS TC046 - Initiate a call using a contact identifier

PASS TC047 - View call history

**FAIL** TC048 - Check call status and outcome during call initiation

An "Accept" or "Reject" button should appear.

PASS TC049 - End the call during call initiation

* **Connection, Notice and Disconnect**

PASS TC050 - Accept incoming call

**FAIL** TC051 - Reject incoming call

Call History will show both Accept and Reject as Called. (Displayed Missed Call if Reject)

**FAIL** TC052 - Missed call notification (call not accepted)

Even if it's a Reject, the duration is displayed as if the call was made

PASS TC053 - Missed call notification (called entity in another call)

PASS TC054 - Call termination notification

PASS TC055 - Application brought to the foreground during incoming call

* **Communication methods**

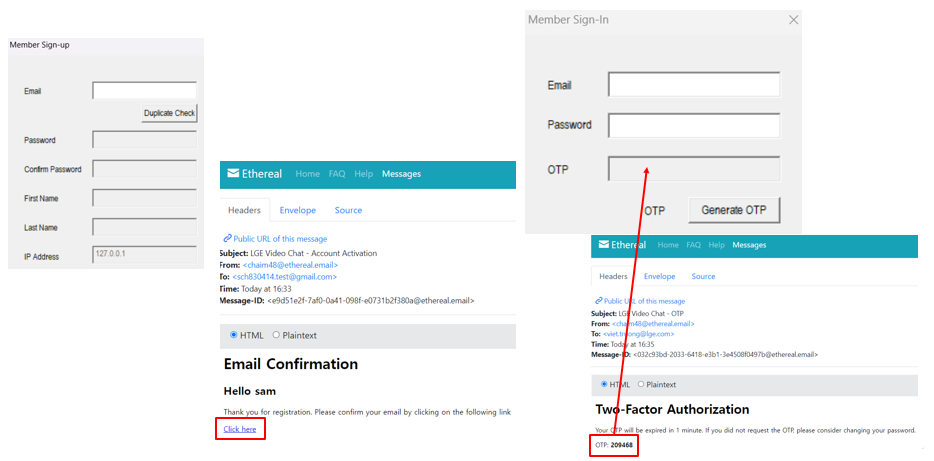
PASS TC056 - Point-to-point communication functionality

PASS TC057 - Call initiation failure

## Verification Result on Security requirements

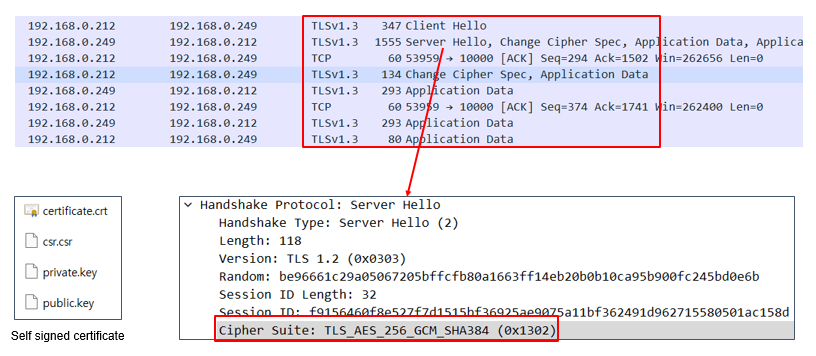
### Two factor authentication

Passed



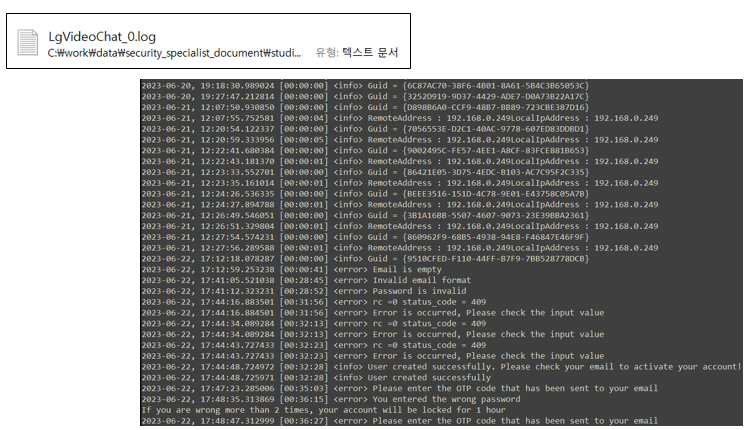
### Server Authentication & Secure communication

Passed



### Storing log file to the file system

Passed



# Lessons Learned

* **Project Plan from Security Perspective**  
  - Our team could understand overall process for the project which has to consider security  
  - To catch up the unexpected needs, our team changed the initial schedule and order
* **Threat Analysis & Secure Design**  
  - Our team was able to realize the importance of threat analysis for secure design  
  - Applying only given requirement by customer can be very dangerous from security perspective  
  - The more we learn and experience on security, the more we could find the threats and mitigations
* **Secure Implementation**  
  - Using open source libraries were essential for our implementation  
  - Not only secure coding but also managing vulnerabilities in the 3rd party libraries will be very important for secure implementation