# SBD Assignment

## Security mechanisms

- Authentication:
    1. Registered phone number
    2. Password checking
    3. Token system
    4. Biometric authentication (fingerprint or face recognition)
- Authorization:
    1. Role-based authorization
- Audit
    1. Protection of log files
    2. Encoding of sensitive data (personal identifiable information, passwords, phone numbers, etc)

## Remarks on why you considered these requirements?

- Authentication:
    1. For granting only the users in this house can access the smart home, we need to register the accounts with their phone number
    2. For users to use the app and access their profiles, they need to authenticate with a pin code / password to prevent unauthorized people from accessing the app through the phone of one of the household members
    3. When users want to register an account or forget the password, we need to use the token to authenticate.
    4. For some advanced authentication features (Optional; could be used for e.g. adding new users or accessing certain sensitive settings)
- authorization:
    1. The admin can register new members and change the settings, others can only control the different smart home components.
- Audit:
    1. To prevent unauthorized user from getting access to personal information through the log files
    2. To prevent people from getting access to this sensitive data in case of a data breach

# Supplement Requirements For Your Application

- Authentication:
    1. Goal:  The system ensure that the SMS code is not simple.
       Requirement: The SMS code is 4 digits and avoids the stupid code such as 0000.
       User story: “As a user, I can enter my phone number and then enter the code sent to me by the application through SMS to access it.
       Abuse case: “As an attacker, I can enter the simple and stupid SMS code to register an account.
    2. Goal: The system verifies that there are no default passwords used by the application or any of its components.
       Requirement:To access the application, one should require authentication.
       User story: “As a user, I can sign in the application by using my username/phone number and password”
       Abuse case: As an attacker, I can enter the default passwords to access the application.
    3. Goal:
       Requirement:
       User story: “As a user, I can get a SMS Token to sign in the application when I forget the password”
       Abuse case:
       (same as 1.)
    4. Goal:
       Requirement:
       User story:
       Abuse case:
- Authorization:
    1. Goal:
       Requirement:
       User story: “As an admin, only I can register the accounts for other users in my family”
       Abuse case:
- Audit:
    1. Goal:
       Requirement:
       User story:
       Abuse case:
    2. Goal:
       Requirement:
       User story:
       Abuse case: ”As an attacker, I can use a brute force method to get access to get the user passwords”

# Risk Identification/Threat Assessment

- Authentication
    1. (1) You enter a wrong phone number more than 3 times. (2) you enter a correct phone number but fail to enter the right passcode
    2. (1) You enter a wrong password more than 3 times. (2) You enter a default password.
    3. (1)
    4. (1) You enter wrong biometric data more than 3 times.
- Authorization:
    1. (1) You try to perform an operation to which you're not authorized twice in a row.
- Audit:
    1. (1) You try to open a log file without the proper permissions
    2. (1) You request sensitive data from the server to which you do not have access