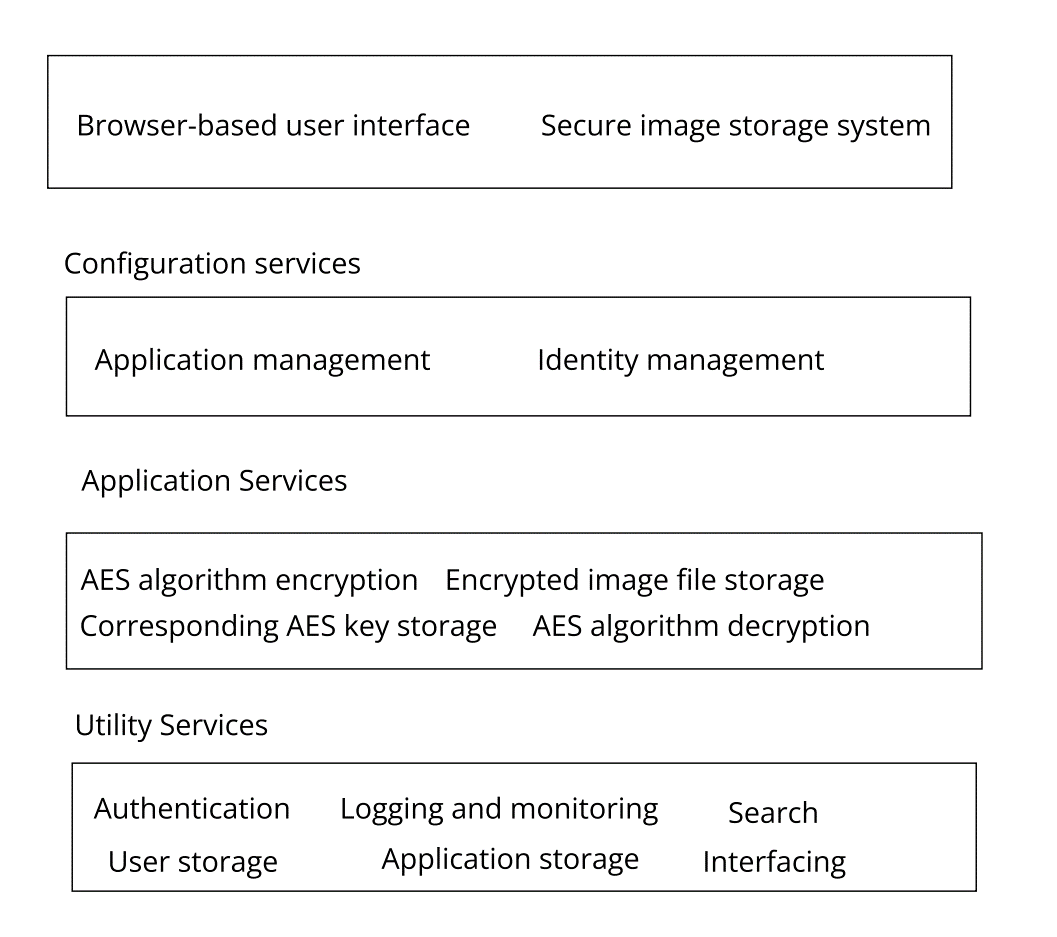
System architecture:

This system can be divided into 4 subsystems based on the functions(cloud-based storage system, AES algorithm system, user information storage system, Authentication handle system).And as we know, layered architecture organizes the system into a set of layers (or abstract machines) each of which provide a set of services. The architecture is also changeable and portable. Because if its interface is unchanged, a new layer with extended functionality can replace an existing layer without changing other parts of the system. So, we choose the layered architecture for this system. This system is divided into 4 layers. The pattern is shown below.



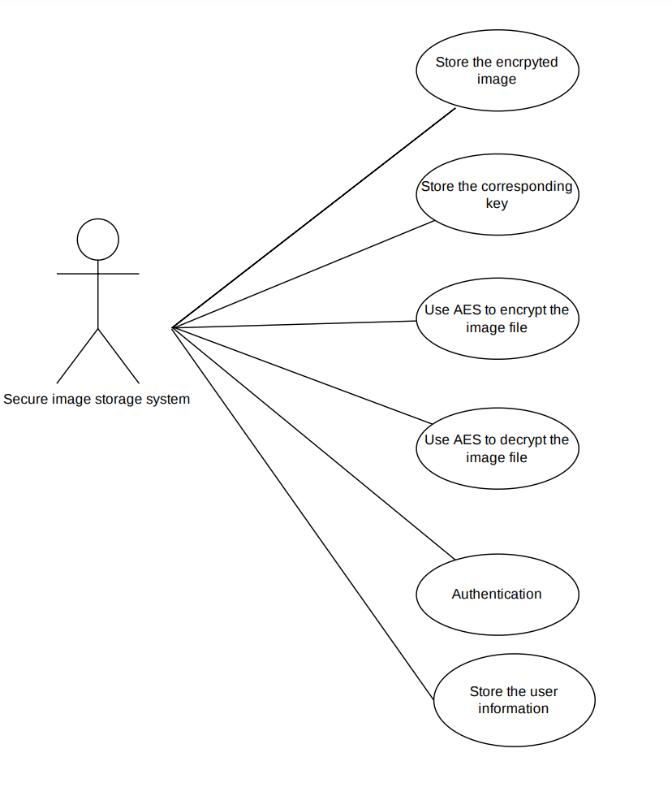
1.The first layer is user interface. This system will have a browser-based user interface. This will give the user the entry to this system and make a connection between these two.

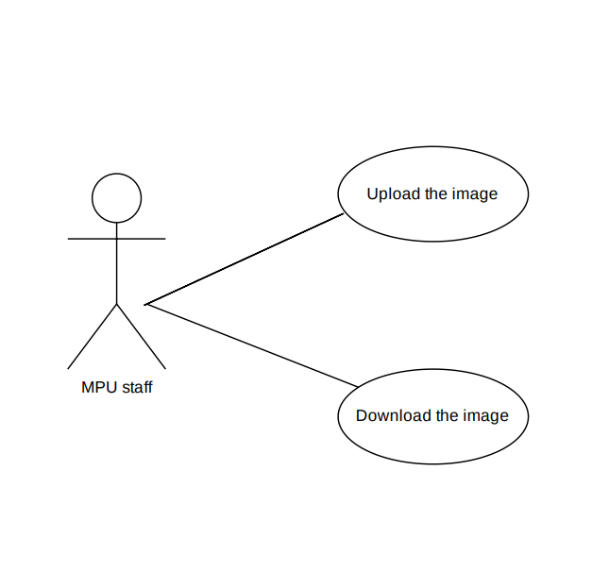
2.The second layer is configuration services. This layer consists of 2 parts: application management and identity management. Application management is about managing and monitoring the application services to make sure them work normally and correctly. Identity management is about managing the user’s identity such as sign up, change the password and so on.

3.The third layer is application services. It contains all the functions that the system provides to the users.

4.The lowest layer is utility services. This is the deepest of this system. It supports above layers.

Use case diagrams

There are 2 actors in this system. The first one is MPU staff. Because they use this system to store the examination paper pictures. The MPU staff can upload and download the image.

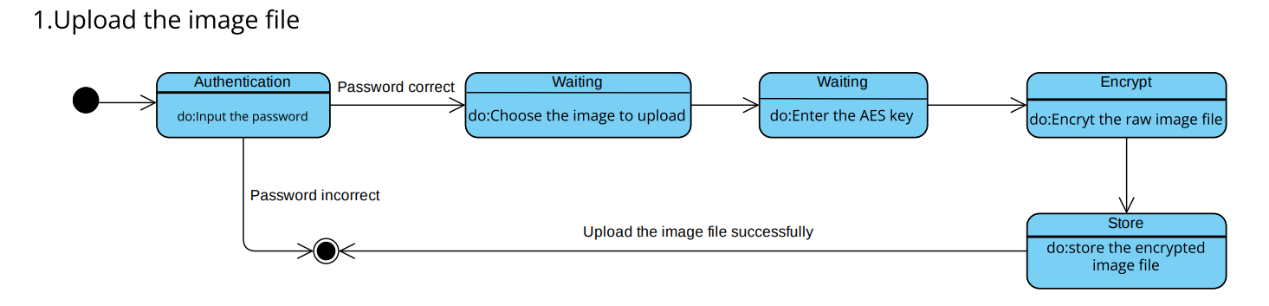


The second actor is the system itself(secure image storage system).The first role the system can play is authentication. Because in the requirement we define only authenticated users can access this system. And it also means that the user needs to input the username and the corresponding password. So, this system also stores the users’ information. The core of this system is about using AES algorithm to encrypt and decrypt the image file. When uploading the image file, the user also needs to enter the key to encrypt the image file. To download the file, the user also needs to enter the key. So, this system not only stores the encrypted image file but also the corresponding key value.

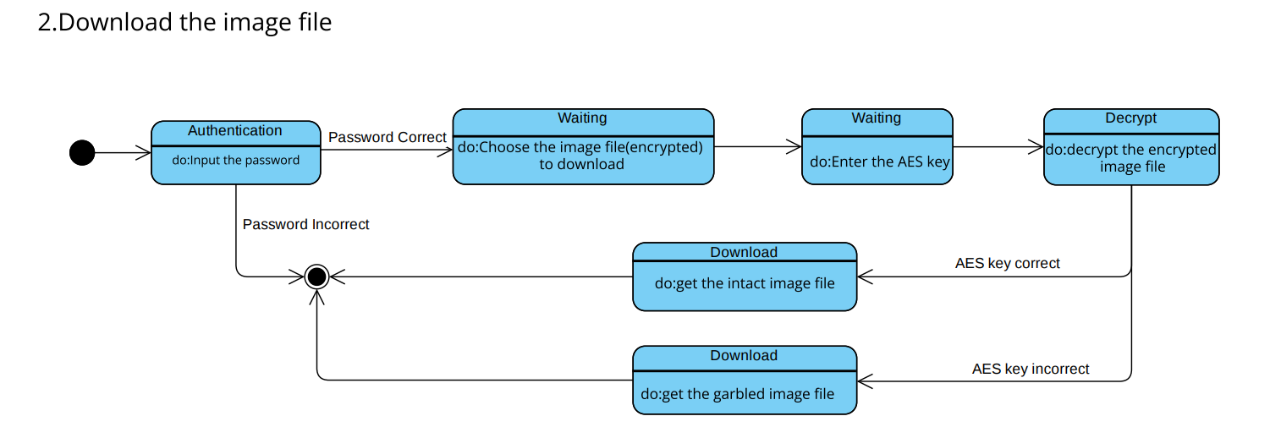
State machine diagram

State machine diagram shows the behaviors of the system in response to external and internal events.

Here we divided this model into 2 parts based on user’s actions.



At the beginning, the user needs to get through the authentication. When they input the correct password, they will enter the system. After they choose the image to upload and enter the key whose format is legal, the system will automatically encrypt the raw image file. In the end, it will store this encrypted image file.



Because download and upload are symmetrical. These first few steps are the same. The major difference is concentrated on the decryption. When the user inputs the wrong key, he will get the garbled image file without being reminded that he made a mistake. Imagine the situation that one malicious user gets through the authentication by accident, he tries inputting the key to get the examination paper image. Without reminding, he will get the gabled file. Maybe he thinks he gets the result and exits the system. This behavior of the system benefits the security a lot.