| **Name:** | **Alvin Tandian** |
| --- | --- |
| **Email:** | **alvin\_tandian@mpa.gov.sg** |

**Question 1**

1. Name a (or more) cryptographic algorithm you would use to perform the following
   1. encryption

**Symmetric Key Algorithm (AES, 3DES)**

* 1. non repudiation

**Asymmetric Key Algorithm (RSA, DSA, ECC) and Hash (SHA256, SHA384, SHA512, bcrypt, scrypt)**

* 1. no tempering

**Hash (SHA256, SHA384, SHA512, bcrypt, scrypt)**

1. Name the following JWT registered claim names (see <https://tools.ietf.org/html/rfc7519#page-9>)
   1. unique JWT identifier

**jti (JWT ID)**

* 1. cannot be used before a certain date

**nbf (Not Before)**

* 1. issue date

**iat (Issued At)**

* 1. token recipient

**aud (Audience)**

* 1. mobile number

**Private Claim Names**

**Question 2**

You are developing a hotel reservation application. After your user have successfully booked a hotel, the application can (opt in) update a user’s Google calendar with the stay’s detail and alerts. The application needs to create, update and delete calendar entries.

What are the required steps to allows the reservation system to update the a user’s calendar?

1. **Application will need to register / create a Google project which will generate API key.**
2. **Using the API key, the application will need to trigger the authorisation with Google Calendar via OAuth 2.0.**
3. **Once user has successfully completed the OAuth 2.0 authorisation, the application will be provided with access token.**
4. **Using the access token, application will be able to trigger the *Events: insert*, *Events: update* and *Events: delete API* to update user’s Google calendar.**

**Question 3**

You and a few friends have co-founded a hot social media startup. Like any good social media startups, you will need a new feed. A news feed is a list of post that is constantly updated with stories, activities, polls, etc from your friends. A post content includes the poster, text, images, videos, simple questionnaires, links, locations, etc.

The post will also include likes, the number of people reacted to it.

Two REST endpoints have been designated for users to publish and retrieve their feeds.

Publish a post

POST /api/v1/feed/me

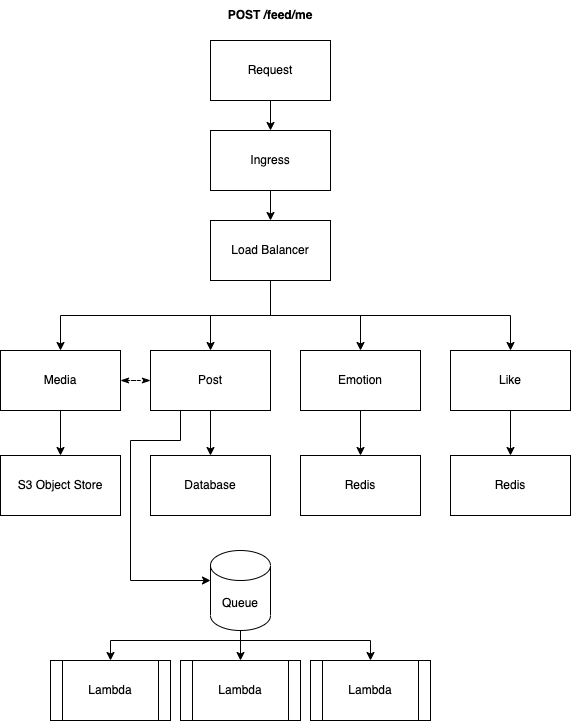
Retrieving a feed

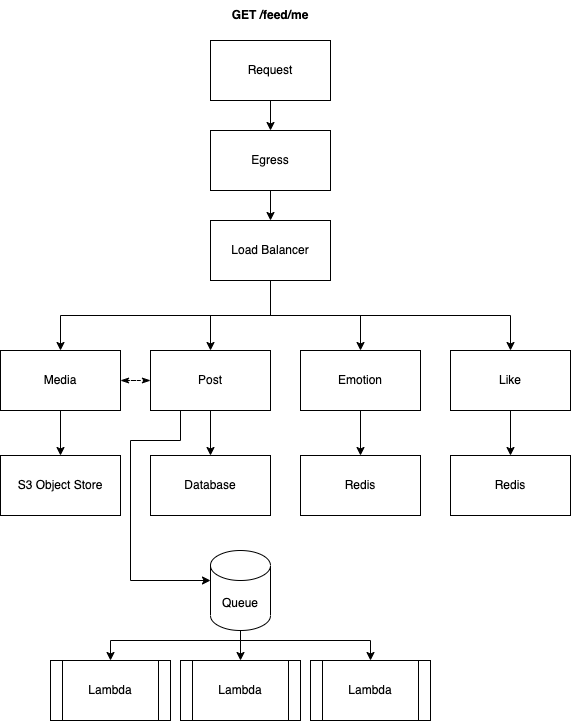
GET /api/v1/feed/me

The endpoints are secured with JWT.

Each user of your social site can have up to a total of 1000 friends/followers. You anticipate 5 million daily active users with about 70% of them posting at least 1 post.

Design a system that will support your REST endpoints along with the given requirements. Be as details a possible with your design.





**Submission**

Copy this Word document to your repository and commit it.

git add .

git commit -m ‘worksheet03’

git push origin master