Report Assignment 3

Table 1

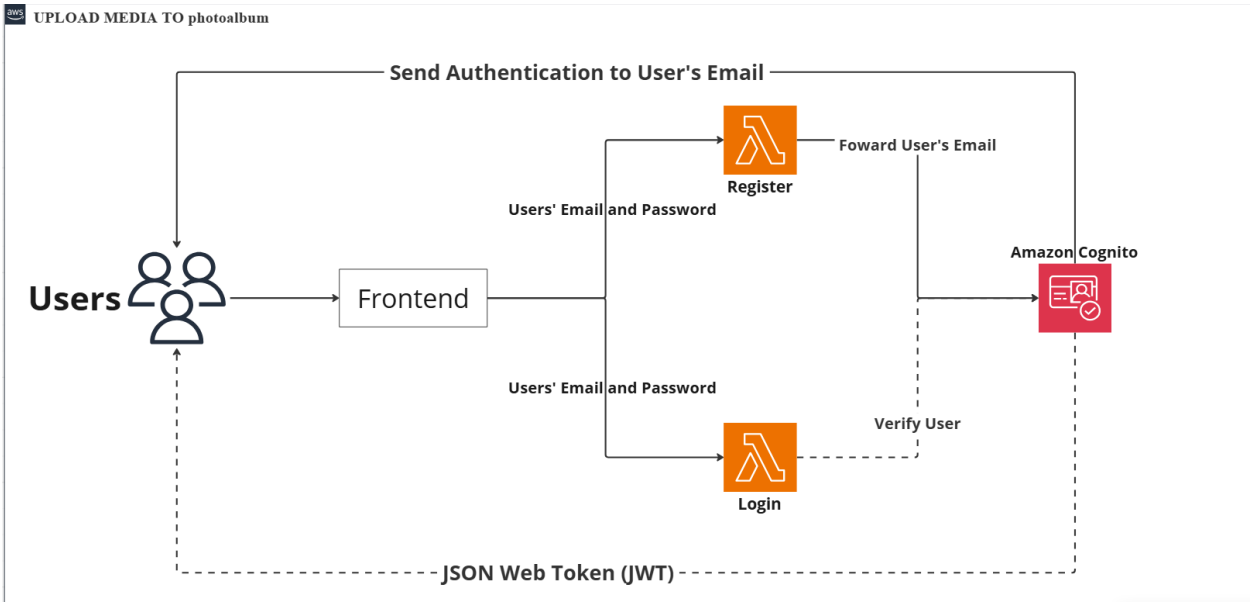

Figure 1. Diagram of User Authentication

Workflow

1. User Interaction with Frontend:
   - The User initiates the process by interacting with the frontend, either to log in or sign up.

2. Frontend Requests to Lambda Functions:
   - Login Request:
     - The User provides their email and password.
     - The frontend sends these credentials to the LOGIN LAMBDA function.
   - Signup Request:
     - The User provides their email and password.
     - The frontend sends these credentials to the SIGNUP LAMBDA function.

3. Lambda Functions Interaction with Amazon Cognito:
   - LOGIN LAMBDA:

    - The function receives the user's email and password and verifies it with a custom format.
    - Then it forwards the user's email and password to Amazon Cognito to verify the user's credentials.
- SIGNUP LAMBDA:
    - The function receives the user's email and password and verifies it with a custom format.
    - Then it forwards the user's email to Amazon Cognito to create a new user account.
- Custom Format to verify:
    - User’s Email: Must be a valid email address
    - User’s Password: Must be 12 characters length include a upper letter, at least a number, a special character.

4. Amazon Cognito:
    - Verification and Authentication:
        - Upon receiving the login request from LOGIN LAMBDA, Cognito verifies the user’s credentials by Cognito User Pools.
        - Upon receiving the signup request from SIGNUP LAMBDA, Cognito creates a new user account (add new user to Cognito User Pools) and sends authentication details to the user's email.

    - Token Generation:
        - After successful verification, Cognito generates a JSON Web Token (JWT) for the user.
        - This JWT is sent back to the User.

5. Completion of the Process:
    - The User receives the JWT.
    - The User can use it to authenticate with the web application as a logged-in user or authenticated user and is then able to legibly request for uploading media to the photoalbum website.

6. Notification to User:
    - Cognito sends authentication details to the user's email as part of the signup process.

DETAILS ON EACH SERVICE IMPLEMENTED IN THE DESIGN

AWS Cognito

- Role: User Authentication and Authorization
- Details:
    - Manages user signup and login.
    - Issues JSON Web Tokens (JWTs) for authenticated sessions.
    - Stores user data (Cognito User Pools) and handles verification processes.

AWS Lambda

- Role: Process the Request from Users
- Details:
    - Login Lambda: Validate user credentials and verify them with AWS Cognito during login.
    - Sign Up Lambda: Validate user registration data and forward it to AWS Cognito for account creation.

COST

UML Sequence Diagram

-Login Phase

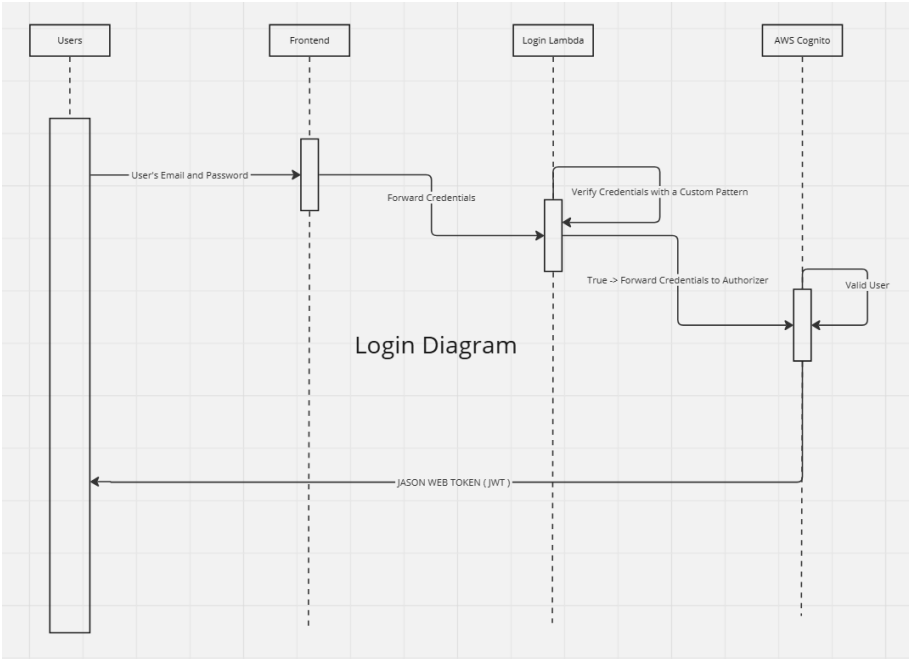

Figure 2 UML Sequence Diagram of Login Process

-Sign-up Phase

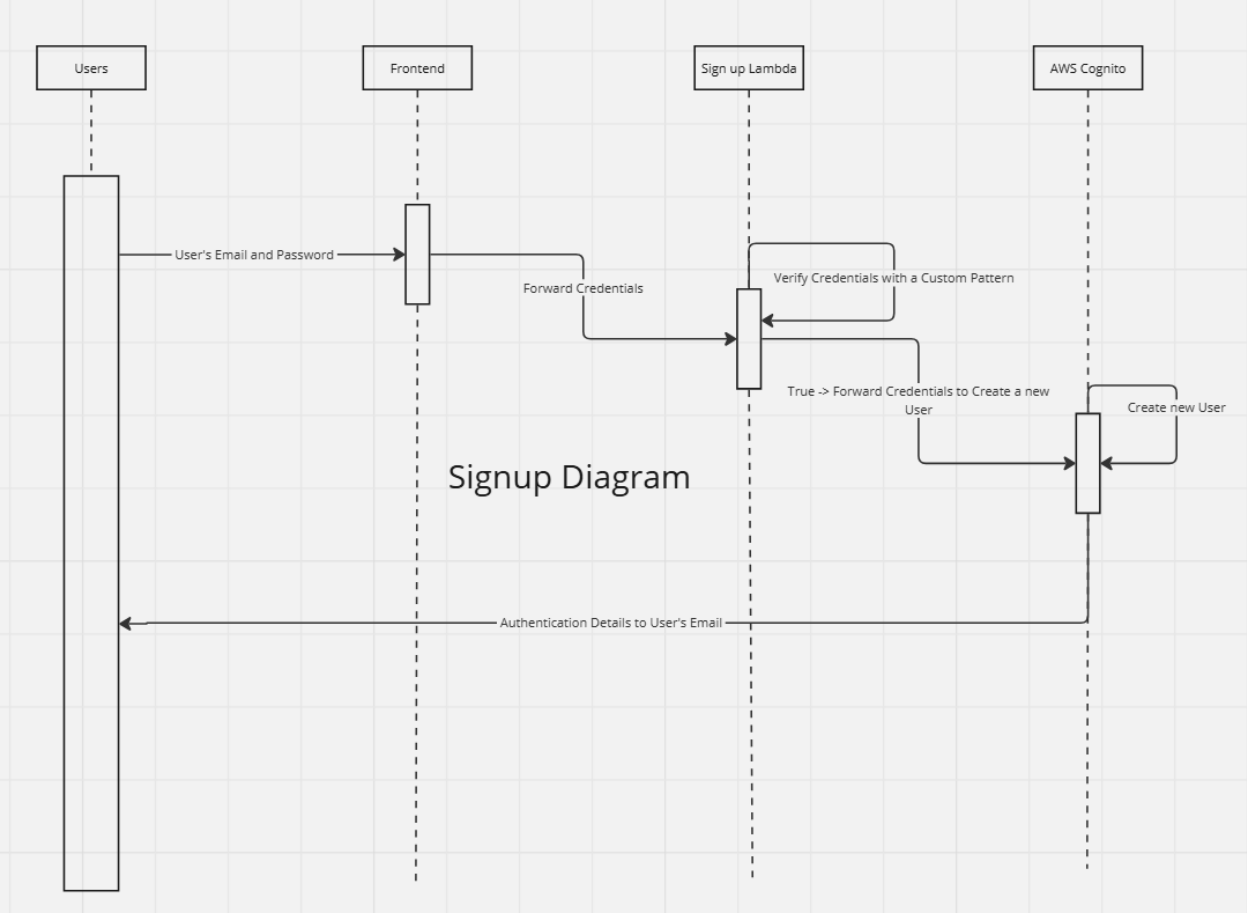

Figure 3 UML Sequence Diagram of Signup Process

Table 2

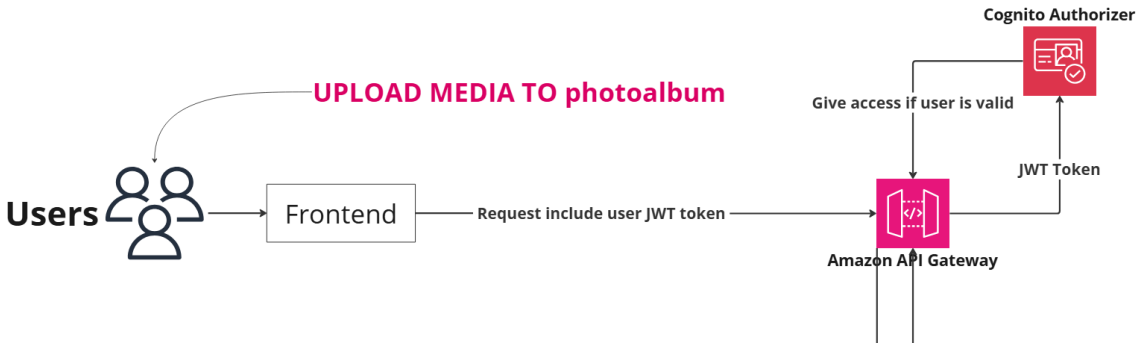

Figure 4 Diagram of authenticated user upload to photoalbum website

Workflow

1. User Upload Media:
   - User interact with the frontend of the photoalbum website to upload media files.

2. Frontend:
   - The frontend collects the media file and includes the user's JWT (JSON Web Token) in the request. The JWT token is obtained during user authentication (Login phase) via Amazon Cognito.

3. Amazon API Gateway:
   - The request from the frontend is sent to Amazon API Gateway, which serves as the entry point for the API. API Gateway handles the incoming requests and routes them to the backend service.
   - API Gateway requires authorization to ensure the request is coming from an authenticated and authorized user.

4. Cognito Authorizer:
   - The JWT token included in the request is validated by the Cognito Authorizer, a feature of API Gateway that integrates with Amazon Cognito.
   - The Cognito Authorizer checks the validity of the token to verify the user's identity and ensure they have the necessary permissions to access the API.
   - If the token is valid, the Cognito Authorizer grants access to the API. If not, access is denied.

5. Backend Processing:
   - Once authorized, API Gateway processes the request and invokes the Lambda function.

DETAILS ON EACH SERVICE IMPLEMENTED IN THE DESIGN

Amazon API Gateway:

- Role: API Management
- Details:
    - API Gateway acts as a front door for photoalbum web application, enabling to secure and route request from frontend to backend. It integrates with Cognito Authorizer for authorization.

Cognito Authorizer:

- Role: Token Validation
- Details:
    - The Cognito Authorizer within API Gateway validates the JWT token provided in the request. It ensures that only authenticated users can access the API.

COST

UML Sequence Diagram

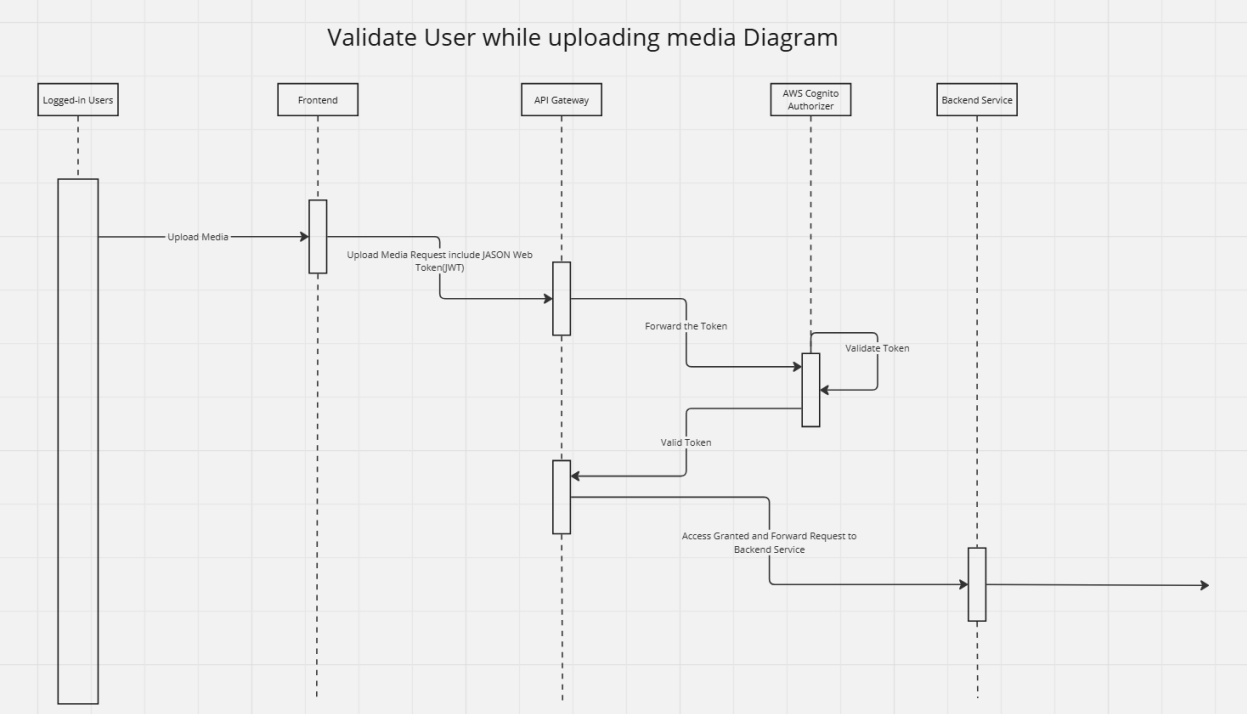

Figure 5 UML Sequence Diagram of Logged-in Users upload media to photoalbum web application

JUSTIFICATION

AWS Cognito - AWS IAM: (Why we using AWS Cognito instead of AWS IAM)

- **Amazon Cognito is ideal for photoalbum web application as it provides seamless user authentication and management, enabling easy sign-up, sign-in, and secure access control for our users. It integrates well with other AWS services, security features without the need for extensive infrastructure management.**
- **User Management:**
    - **Amazon Cognito: Provides user pools for managing user directories and identity pools for obtaining temporary AWS credentials. It handles user registration, authentication, and account recovery.**
    - **AWS IAM: Manages AWS account users, groups, and roles. It does not manage application-specific users or provide authentication services for web/mobile apps.**
- **Authentication:**
    - **Amazon Cognito: Supports various authentication methods, including username/password, social logins (Facebook, Google), and SAML-based identity providers. It also supports multi-factor authentication (MFA).**
    - **AWS IAM: Authentication is primarily for AWS users via access keys, secret keys, and MFA for securing access to AWS services.**