COS20019 Cloud Computing Architecture – Assignment 1b

Lorraine Becker
Student ID: 104584773
Tutorial: 08:30 Thursday
Swinburne University of Technology
Melbourne, Australia
104584773@student.swin.edu.au

***Abstract*— Creating and deploying a Photo Album website onto a simple AWS infrastructure.**

Links:
- Album.php:
http://54.227.85.132/cos20019/photoalbum/album.php

- phpMyAdmin:
http://ec2-54-227-85-132.compute-1.amazonaws.com/phpmyadmin/index.php

***Keywords* — cloud architecture, deployment, technology**

I. Introduction

Assignment 1b of COS20019 Cloud Computing Architecture entails the development and deployment of a photo album website on simple Amazon Web Services (AWS) infrastructure. The infrastructure deployment is illustrated in the following diagram:

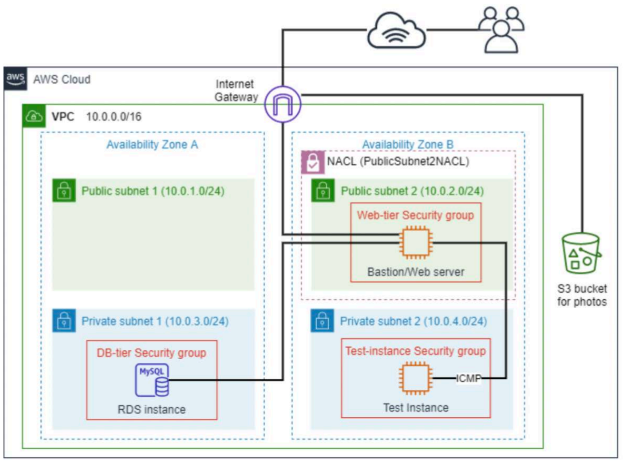

Fig. 1 System Architecture Diagram

Infrastructure Deployment

A secure Virtual Private Cloud (VPC) has been created, and the services required for this assignment were allocated within this VPC.

I. VPC

The VPC has been named LBeckerVPC. It was configured in the us-east-1 region and consists of two availability zones, each with a private and public subnet which follow the appropriate CIDR blocks specified in Figure 1.

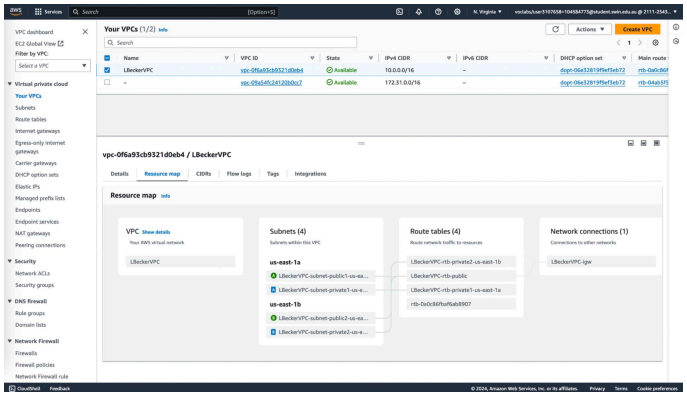

Fig. 2 Created VPC

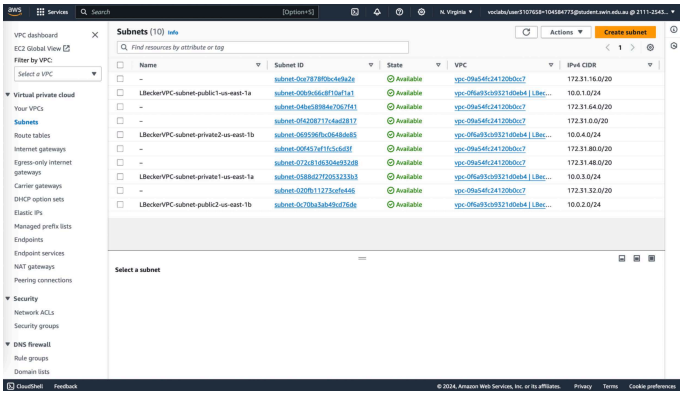

Fig. 3 Created subnets for VPC

The public subnets have been associated with a public route table configured to route traffic to the Internet Gateway. Conversely, the private route tables do not have an Internet gateway configuration. (Fig. 4).

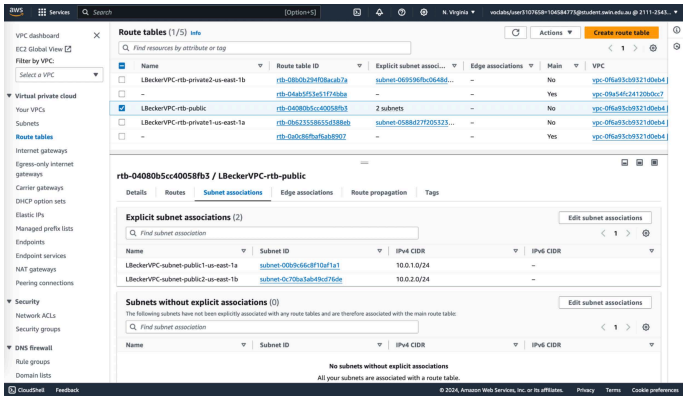

Fig. 4 Subnet associations of the public route table

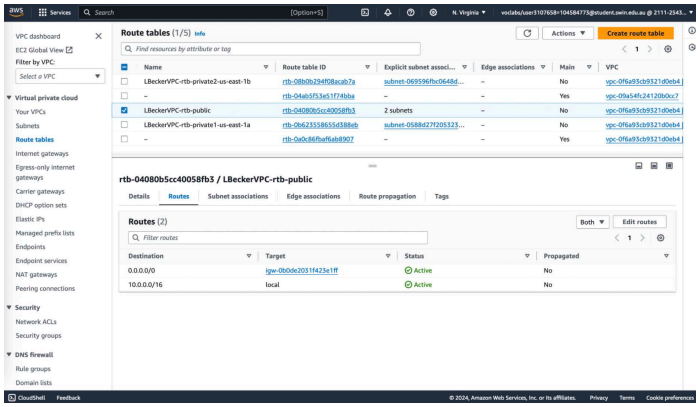

Fig. 5 Routes of public route table

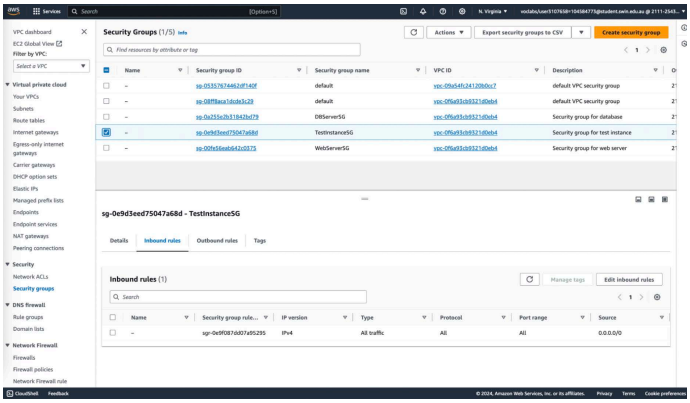

Fig. 8 TestInstanceSG Security Group

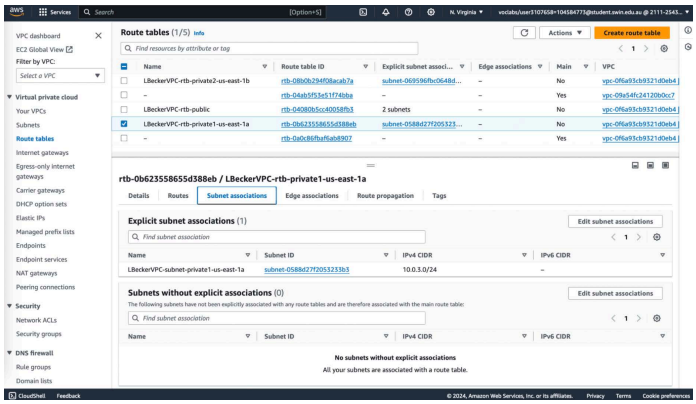

Fig. 6 Subnet associations of Private subnet 1

WebServerSG has three inbound rules:

- Permits HTTP (port 80) traffic from any source.
- Permits SSH (port 22) traffic from any source.
- Permits all ICMP traffic from the security group TestInstanceSG.

In a home environment, the IP address can change at anymoment, therefore it is not reliable to depend on a single source. However, it is advisable to restrict SSH access to specific IP address ranges, such as those within an admin subnet of a business network.

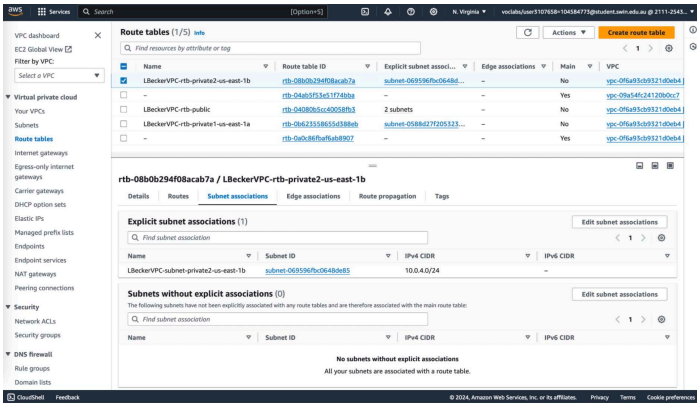

Fig. 7 Subnet associations of Private subnet 2

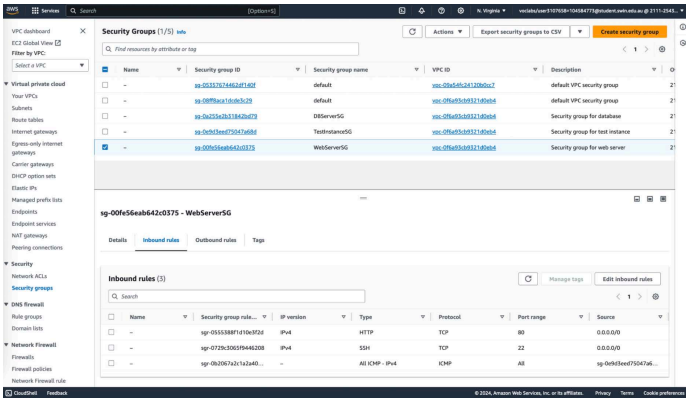

Fig. 9 WebServerSG Security Group

II. SECURITY GROUPS

Security groups were created as depicted in Figure 1, with each one being configured with a specific set of rules.
TestInstanceSG has an inbound rule which permits all traffic attempting to access the resources associated with it.

DBServerSG is configured with an inbound rule that allows MySQL access from the WebServerSG security group. Access from any other sources is restricted.

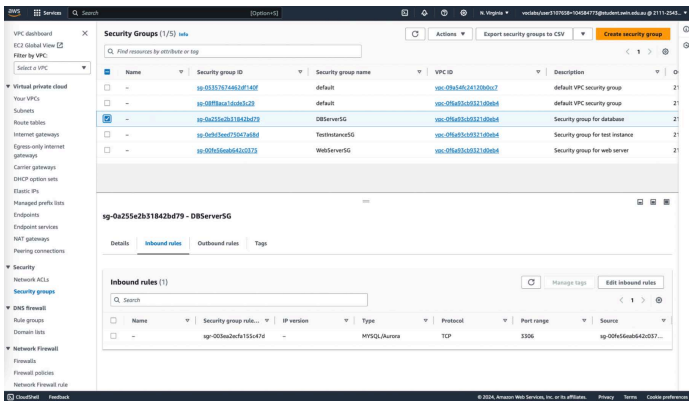

Fig. 10 DBServerSG Security Group

Two EC2 instances were created. The Web Server Instance was placed in the public subnet in order to make it publicly accessible. The Web Server is assigned an elastic IP address, providing it with a static IP address. This allows for easy access to the Web Server, such as establishing an SSH session, through the static IP address, saving time. As the IP address does not require any changes, this implies that the IP address can be used for an A record on the domain.

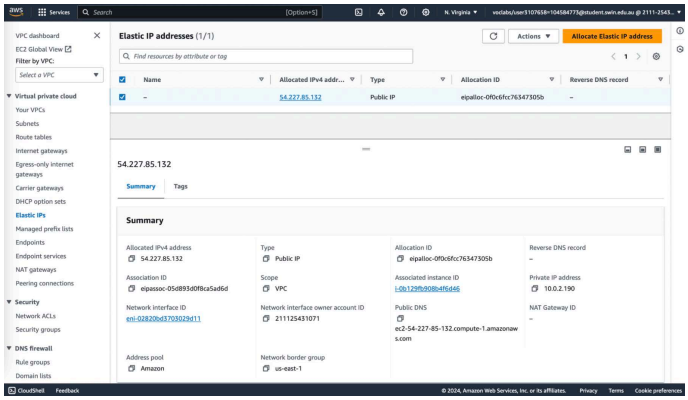

Fig. 11 Elastic IP address

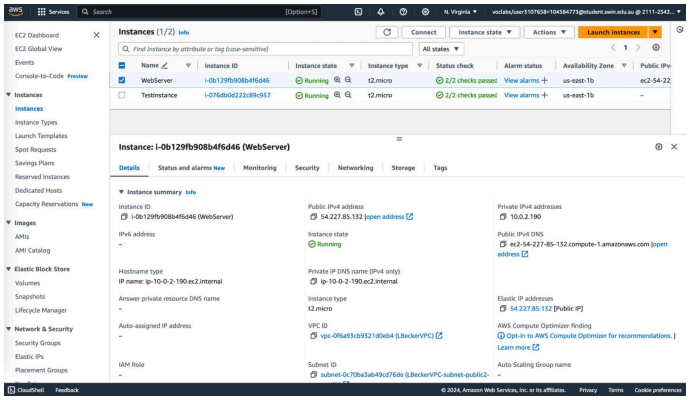

Fig. 12 Web Server EC2 Instance

Fig. 13 Establish an SSH connection to both the Web Server and the Test Instance, then ping the Web Server from the Test Instance.

An SSH connection was successfully created with the Web Server. Using agent forwarding through the Mac terminal, another SSH connection was made from the Web Server to the Test Instance. The Server was tested by pinging the Web Server from the Test Instance. Ultimately, the Web Server's ICMP rule was verified through the server's connectivity.

IV. RDS Database Instance

An instance of Amazon Relational Database Service (RDS) named "photoalbum-db" has been established to serve as the host for the photo album database, which includes a table dedicated to storing photo metadata. Following this setup, the PHP application accesses the "photos" table. Security measures include associating the RDS instance with the "DBServerSG" security group, which permits MySQL traffic from the "WebServerSG" security group. This setup ensures secure communication between the Web Server instance and the database. Additionally, the RDS instance's subnet group is configured to use the VPC's two private subnets.

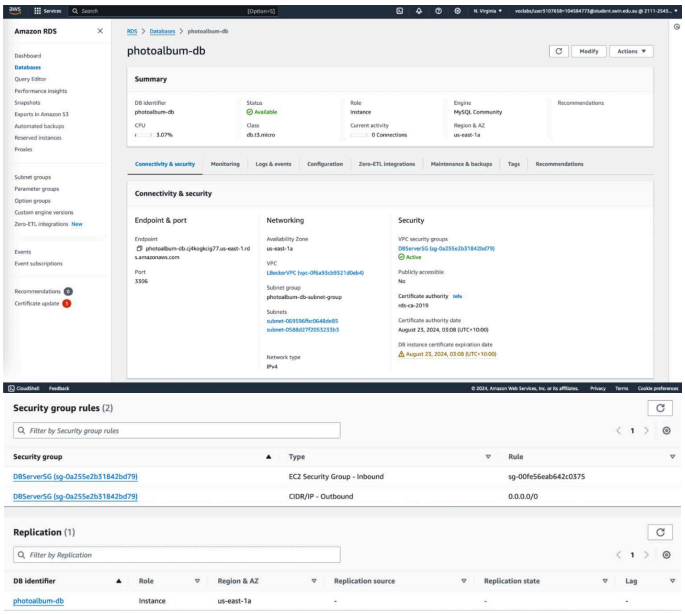

Fig. 14 Photo Album RDS Instance

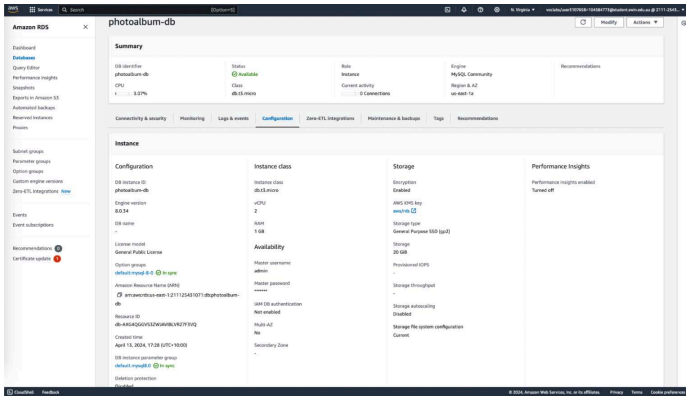

Fig. 15 Configuration of the Photo Album RDS Instance.

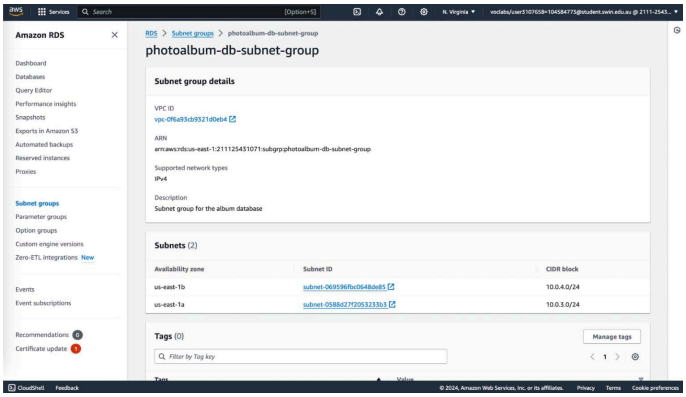

Fig. 16 Subnet group configuration for the Photo Album RDS Instance.

I created a photos table in my photoalbum database on the RDS instance, then added some data to it using phpMyAdmin on the Web Server instance. I connected phpMyAdmin to the RDS instance using its endpoint address.

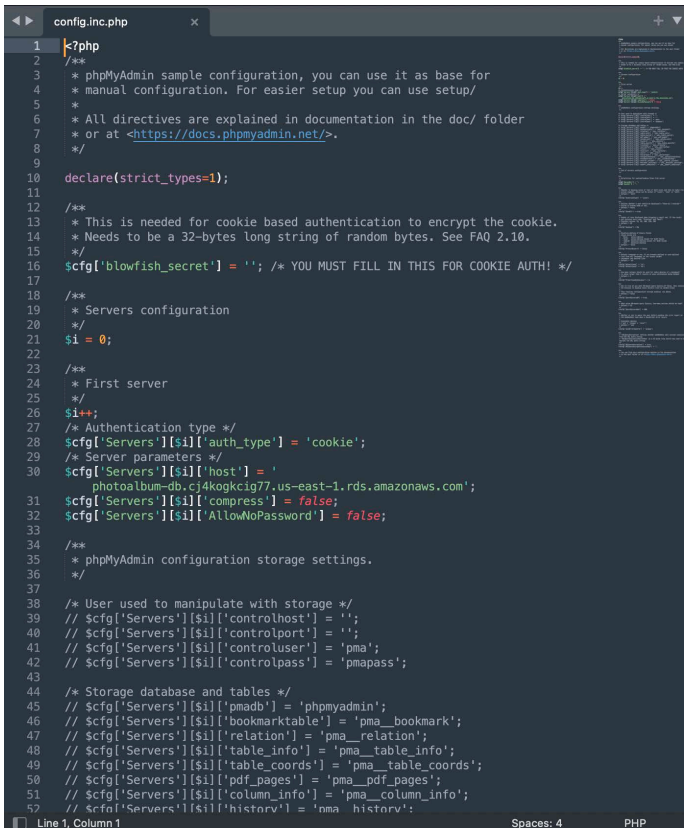

Fig. 17 phpMyAdmin configuration

phpMyAdmin was then accessed through a web browser using the public address of the Web Server instance. The required “photos” table was created with the required columns to store photo metadata. Data was added at a later stage.

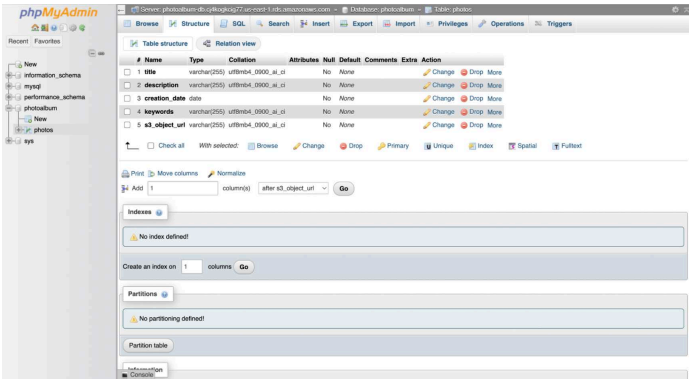

Fig. 18 Creation of the table structure using phpMyAdmin.

- Virtual Network ACLs:

Network Access Control List Creation:

- A Network Access Control List (NACL) named "PublicSubnet2NACL" was created with the following rules:
- Allow SSH traffic from anywhere.
- Allow ICMP traffic only from the Test Instance’s subnet (10.0.4.0/24).
- Allow other traffic to ensure the complete functionality of the Photo Album website for users accessing it from anywhere.

Inbound Rules for NACL:

- **Rule 10:** Authorize HTTP (port 80) access from any location, guaranteeing global accessibility to the photo album site hosted on the Web Server.
- **Rules 20 and 30:** Allow the ephemeral port range [2] to support MySQL connections within the subnets of the database subnet group. Additionally, Rule 30 facilitates SSH outgoing connections from the Web Server to the Test Instance via this port range.
- **Rule 40:** Explicitly permit SSH from any source. Although not ideal, it's necessary for operational purposes, as specifying specific sources for SSH access isn't feasible.
- **Rule 50:** Permit ICMP from private subnet 2, which accommodates the Test Instance, enabling it to ping the Web Server.
- **Rule 60:** Restrict ICMP traffic from any source outside the designated private subnet, ensuring security by denying access from unauthorized locations.

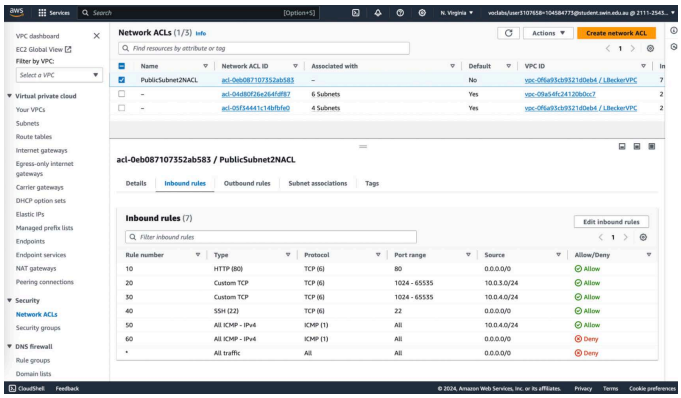

Fig. 19 PublicSubnet2NACL inbound rules

In the outbound rules, a rule was added to allow traffic from any source. This rule overrides the default rule that denies all traffic. Without this change, only incoming traffic would be permitted, while outbound communication would be restricted, resulting in one-way communication

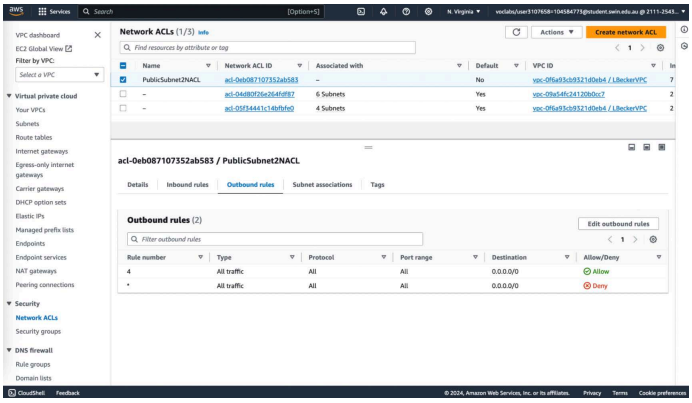

Fig. 20 Outbound rules for PublicSubnet2NACL

FUNCTIONAL REQUIREMNTS FOR THE PHOTO ALBUM WEBSITE

I. S3 bucket

In the us-east-1 region, a bucket named 'lbecker-photoalbum-bucket" was created. The bucket is dedicated to storing photos for the photo album website. Additionally, a policy was implemented to enable public access within the bucket.

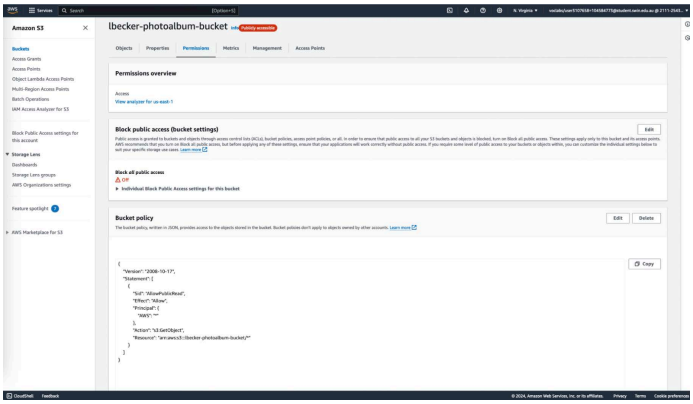

Fig. 21 S3 bucket policy

II. Added rows to the photo table

For testing, more rows were added to the photos table within the RDS instance's photoalbum database. Each entry included URLs for each photo, which point to the bucket, then added to the table.

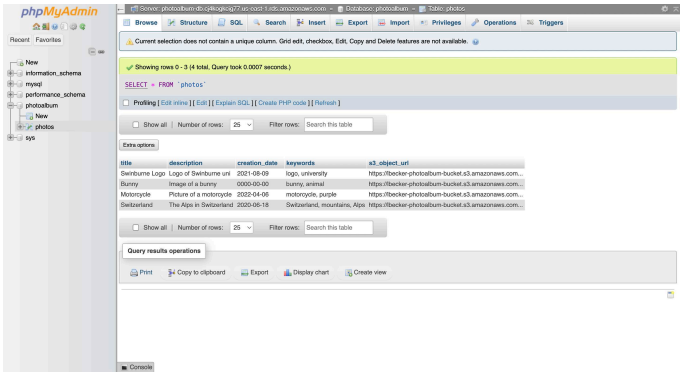

Fig. 22 Photos table with several records of data

The source files of the photo album were transferred to the Web Server instance via SFTP using Cyberduck on a Mac system.

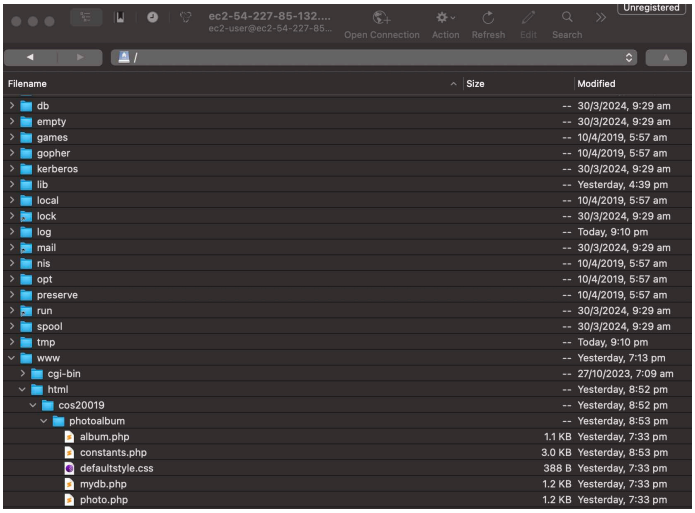

Fig. 23 Transferred source files to Web Server

The constants.php file was altered to incorporate details associated with the database such as the RDS's endpoint address, database name, and column names. These adjustments specify the location of the photos and dictate which columns to use for presenting information. Upon accessing album.php from a web browser, images are shown as expected by retrieving each image through its corresponding URL from the S3 bucket.

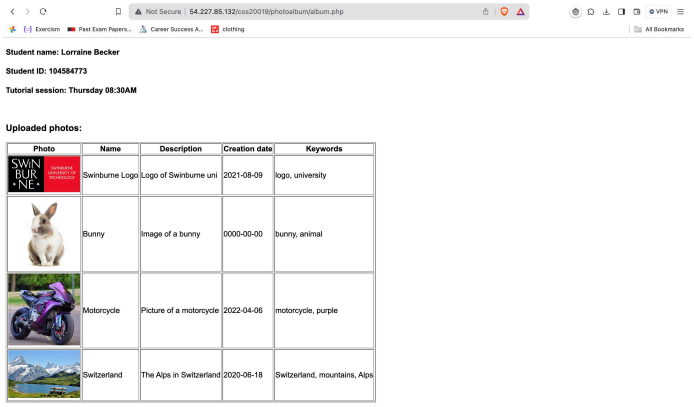

Fig. 24 Accessing album.php via the web browser over the Internet

CONCLUSION

Amazon Web Services offers robust and flexible infrastructure and tools for creating cloud-based systems. The Photo Album website was launched on AWS by using AWS EC2 for the Web Server, RDS for the photo metadata, S3 for storing the image files, and the implementation of Network ACLs to enhance the web server's security.

REFERENCES

[1] Swinburne University, “https://swinburne.instructure.com/courses/56945/modules” 2024. [Online].

[2] “Ephemeral port selection,” www.ibm.com. “https://www.ibm.com/docs/en/zos/3.1.0?topic=profiletcpip-ephemeral-port-selection” 2021. [Online]