Assignment 1B Checklist

Make sure all the following are completed.

Submission Checklist

Student Name: Nhat Minh Tran

Student Id: 104082552

Tutorial time: Tuesday, 6.30-8.30pm

Date of submission: 17/09/2023

Submit to Canvas:

A PDF document file as specified in the Submission section of the assignment specification.

Marking Scheme

Infrastructure Requirements		
VPC with 2 public and 2 private subnets	.5	**Done**
Correct Public and Private Routing tables with correct subnet associations	1	**Done**
Security groups properly configured and attached.	1	**Done**
Network ACL properly configured and attached	1.5	**Done**
Correct Web server and Test instances running in correct subnets	.5	**Done**
Database schema as specified	.5	**Done**
Database running in correct subnets	1	**Done**
S3 objects publicly accessible, using proper access policy	.5	**Done**
Functional Requirements		
album.php page displayed from EC2 Web server	1	**Done**
Provided URL is persistent (Elastic IP Association)	.5	**Done**
Photos loaded from S3 with matching metadata from RDS	1	**Done**
Web server instance reachable from Test instance via ICMP	1	**Done**
Deductions		
Documentation not as specified or poorly presented (up to minus 20)		
Serious misconfigurations of AWS services being used (up to minus 20)		

1. Infrastructure deployment

1.1 – VPC

In the first stage, I created a VPC. Secondly, following the diagram in the assignment, I created four subnets in two AZs. IGW is created and attached to VPC, it also associated to public route table.

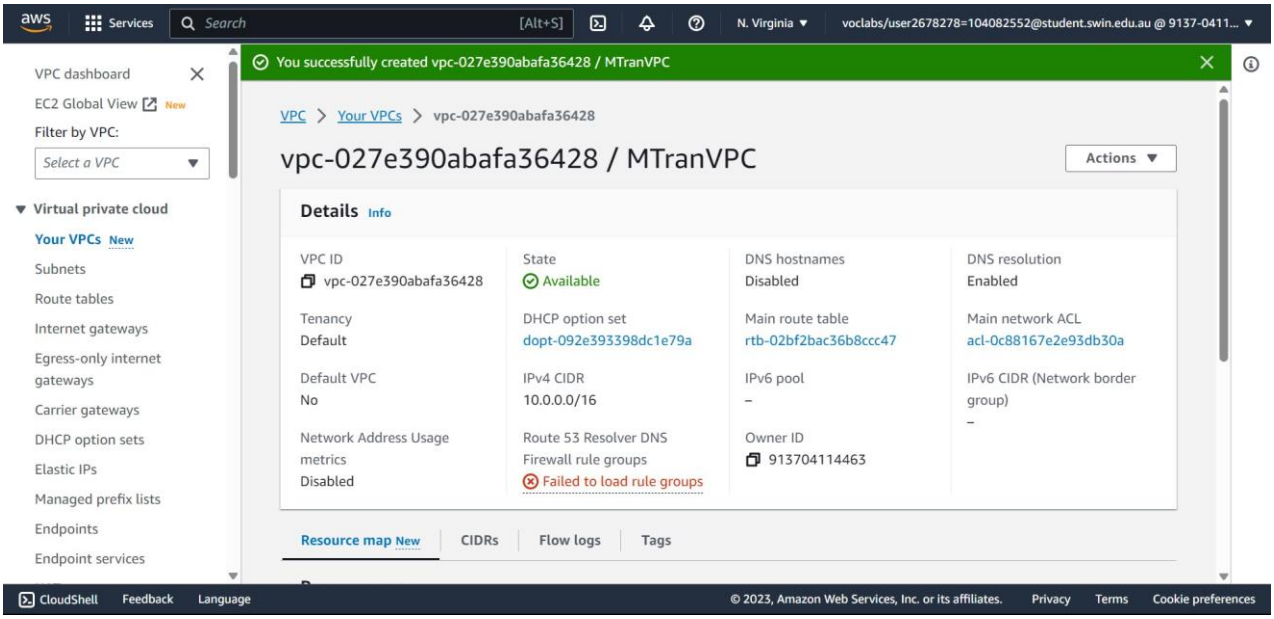

Figure 1: VPC created

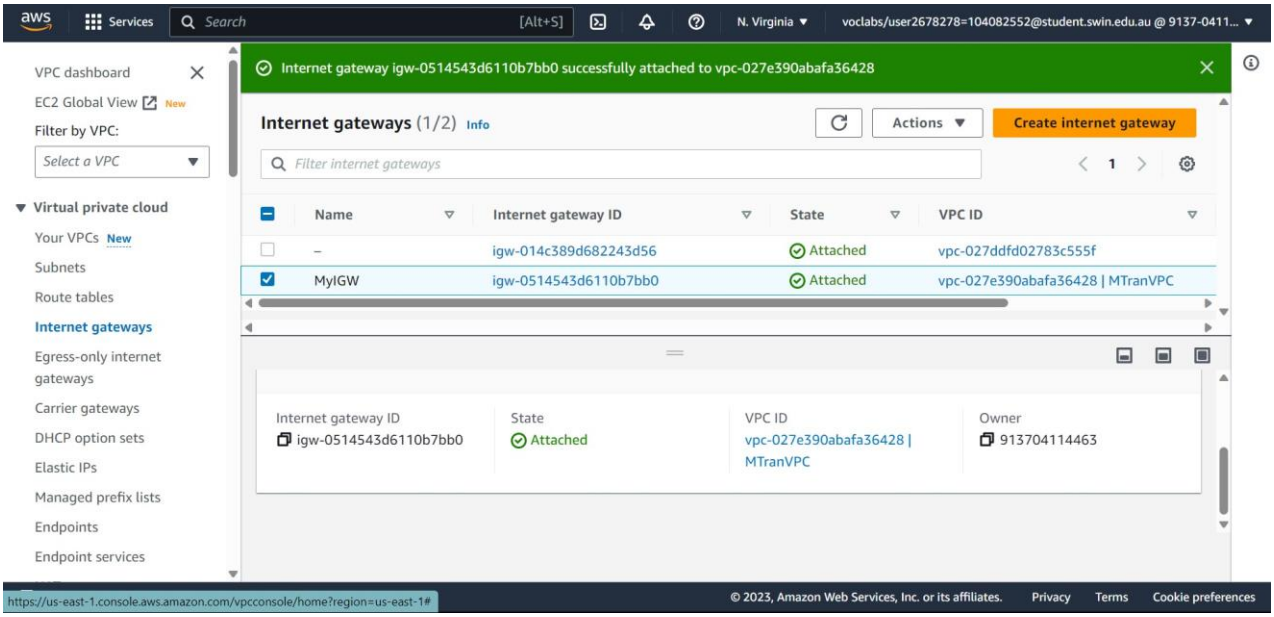

Figure 2: IGW is attached to MTran VPC

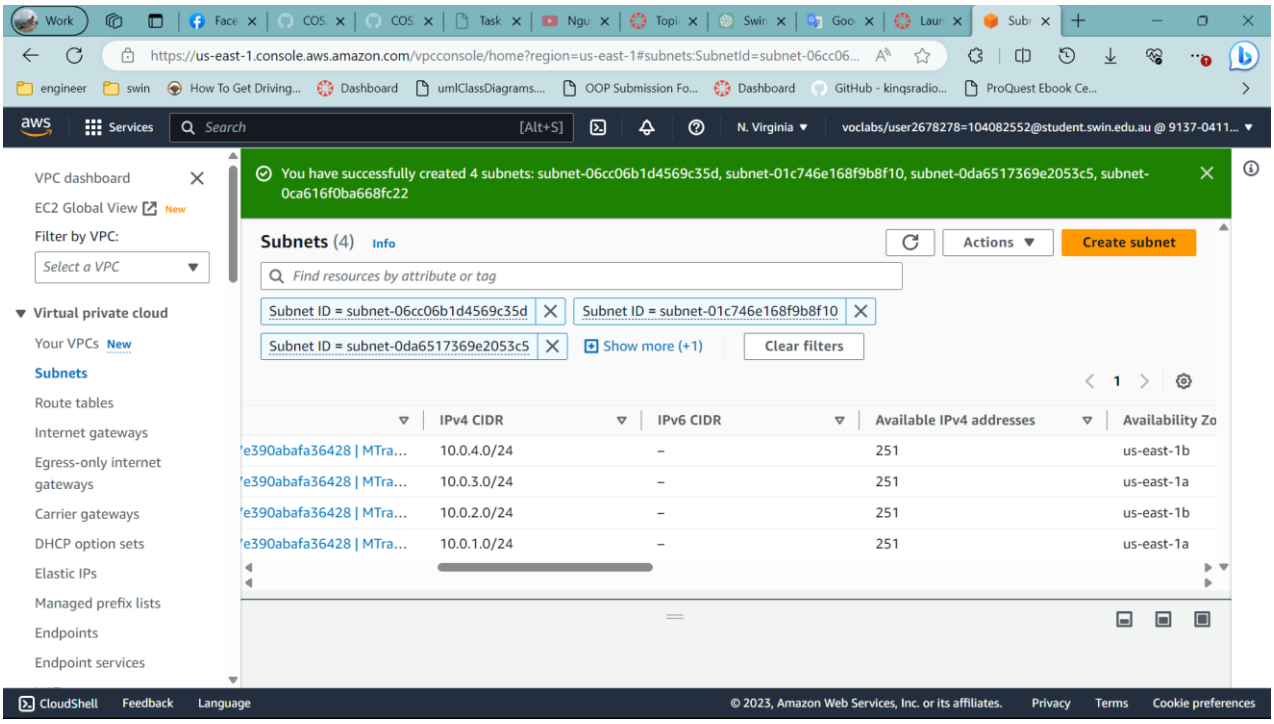

Figure 3: 4 subnets with 2 AZs

There are four subnets(two public and two private), for this assignment, the subnet public 2 will attached to IGW, the subnet public 1 is created but will not be used.

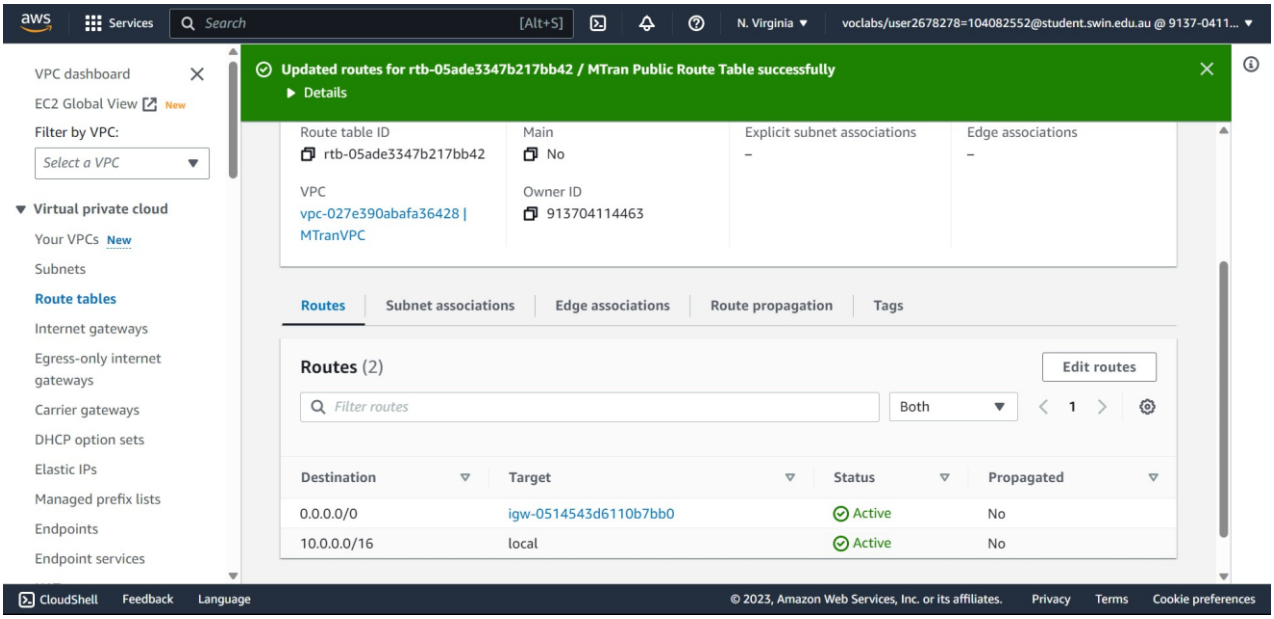

Figure 4: Public route table

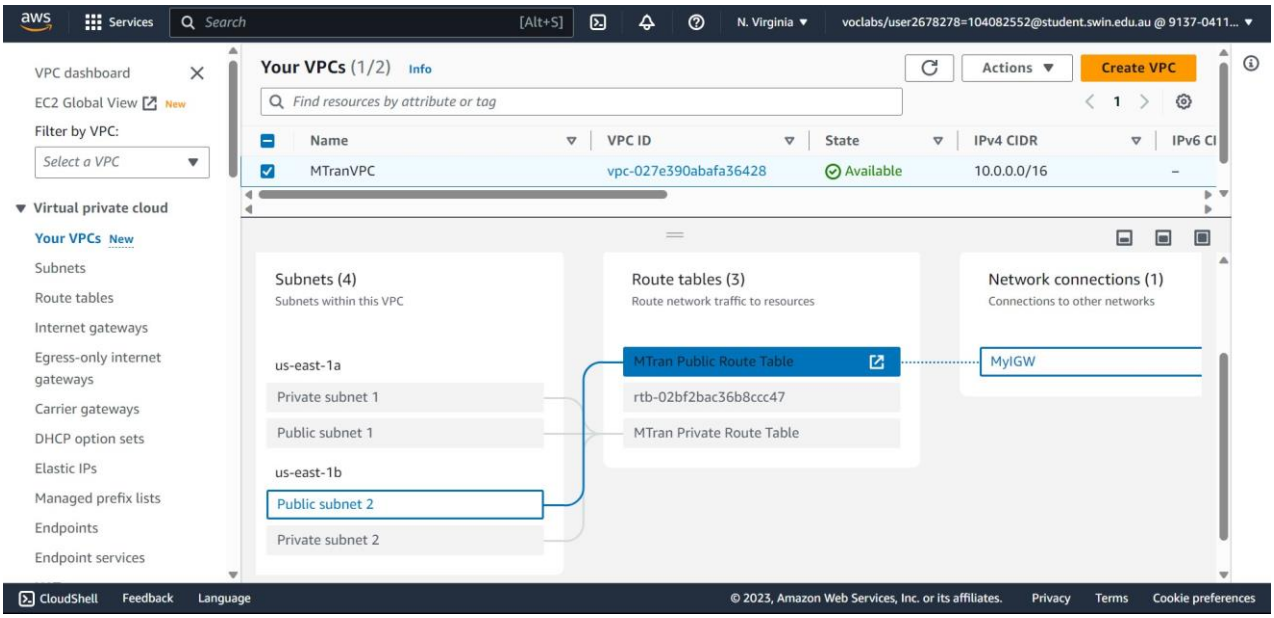

Figure 5: Resource maps

Route table determines where network traffic is directed. Each subnet in VPC will be associated with a route table. This determines which route table rules apply to the traffic in that subnet. In this scenario, only public subnet 2 goes through public table and IGW, while other three are associated to private route table.

1.2 – Security groups

Three security groups are built with different protocols to allow specific instances. These are all assigned with MTranVPC.

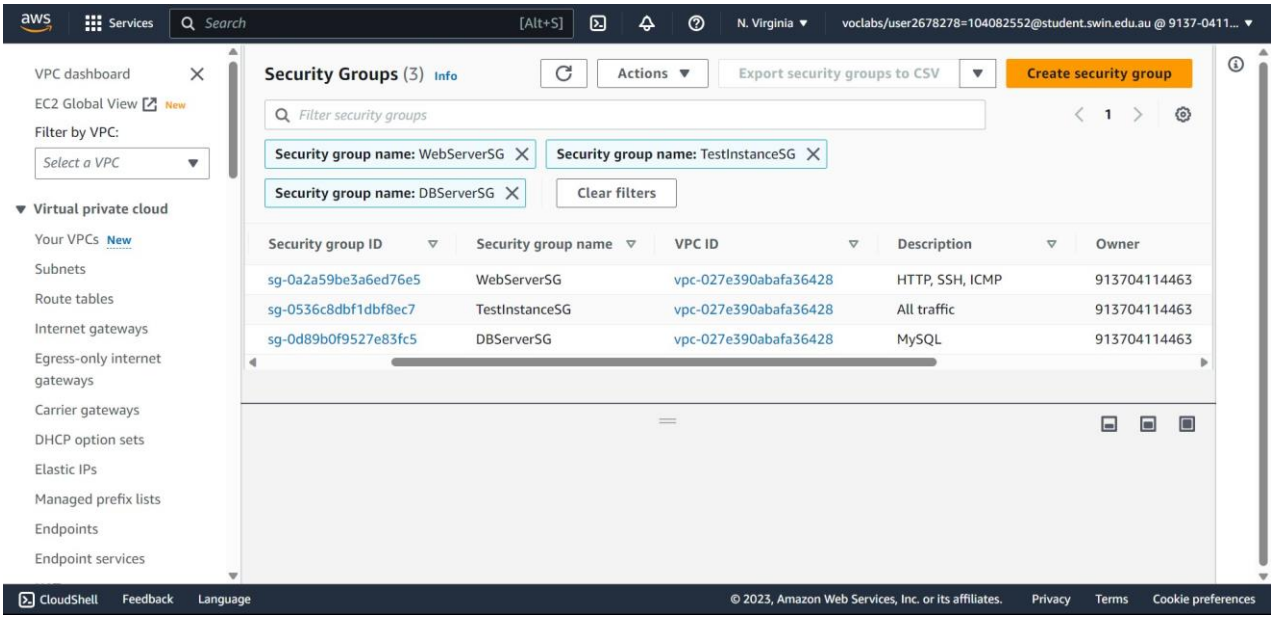

Figure 6: 3 security group

1.3 – EC2 virtual machine

In this stage, I created two EC2 instances, a web server instance and a test instance. The web server instance had PHP/HTML code to run the website. VPC is associated with Elastic Ip so that it is fixed.

Elastic IP provides a static, public IPv4 that you can assign to your AWS. The most important is that the elastic IP does not change every time you start or end lab.

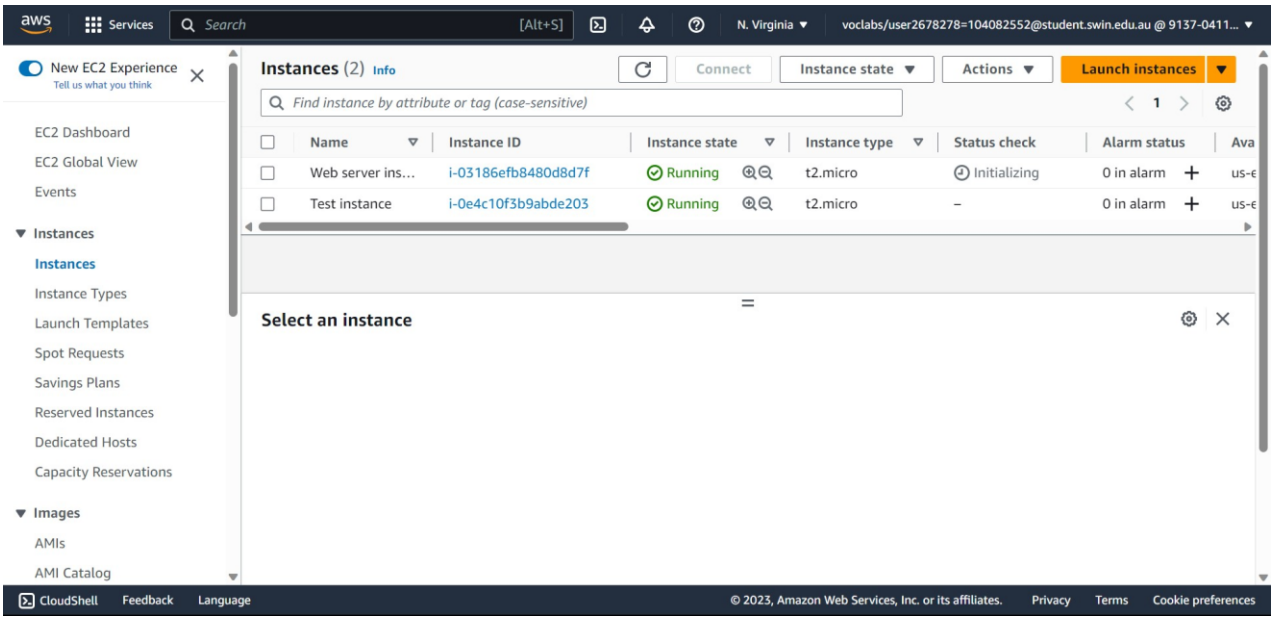

Figure 7: Web server instance and Test instance

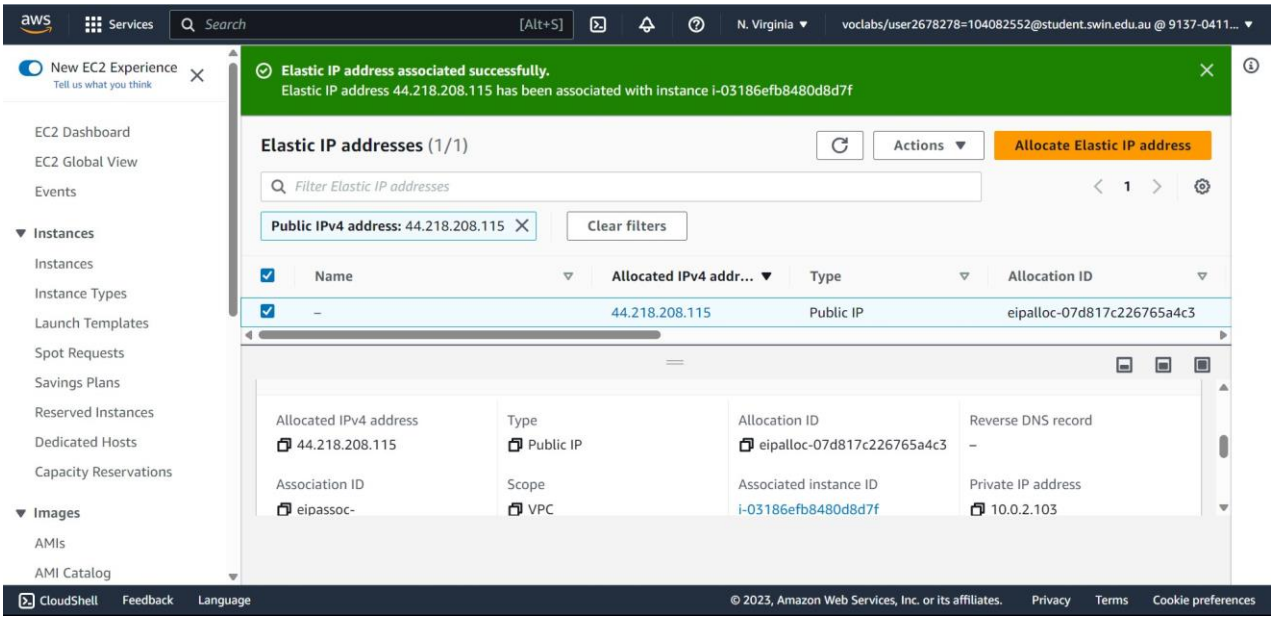

Figure 8: Elastic Ip for Web server instance

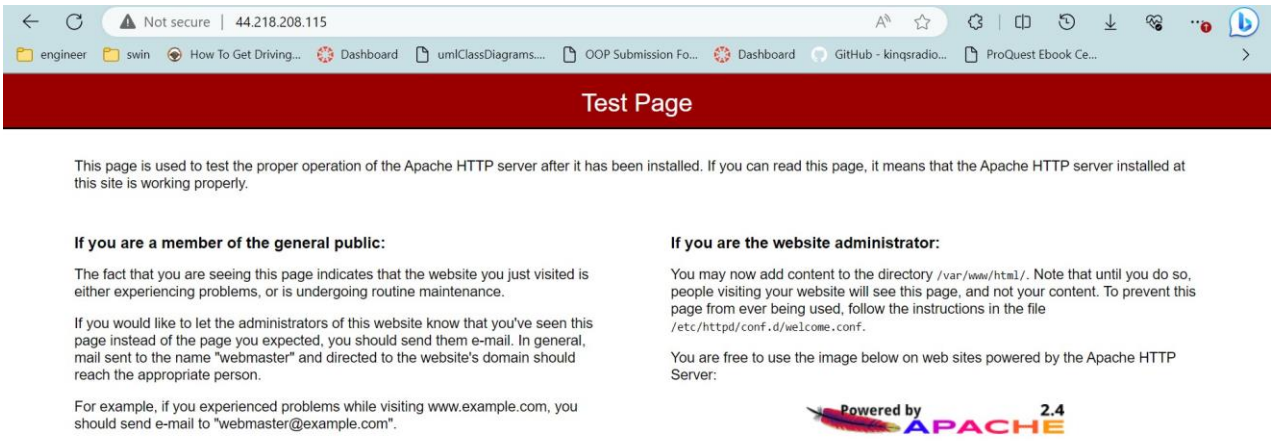

Figure 9: Test webpage with elastic IP

1.4 – RDS database instance

The database service is the service that cannot be visible to the customers. In order to do that, this instance must be in a private subnet in the VPC. However, the RDS instance needs to be access over the internet for setup and maintenance purposes. This can be done by installing phpMyAdmin The security group “DBServerSG” has also been associated with this instance. This setup creates many layers for security purposes and reduce the chance of being exposure to the public internet.

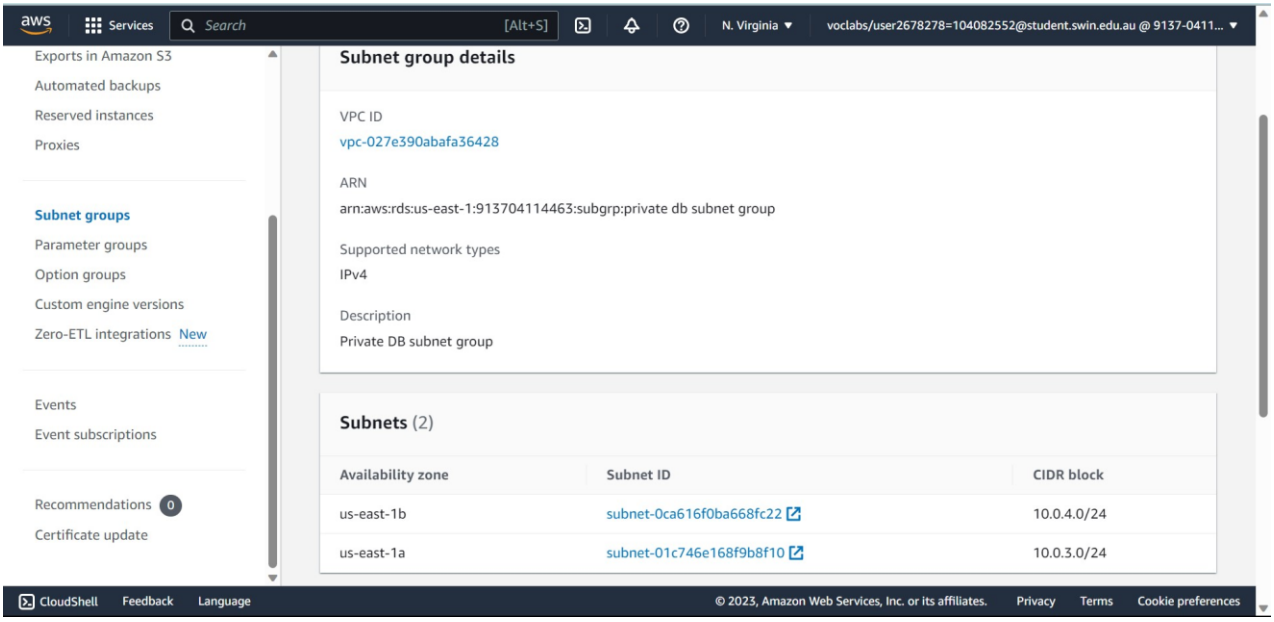

Figure 10: Subnet groups for RDS

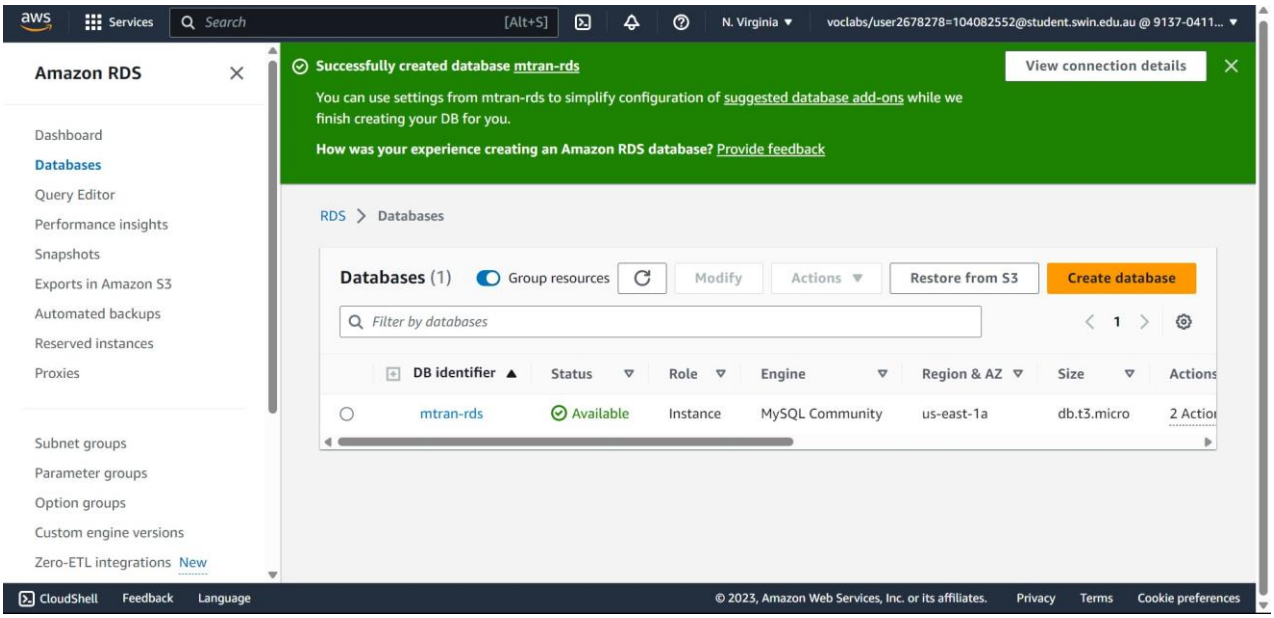

Figure 11: RDS instance

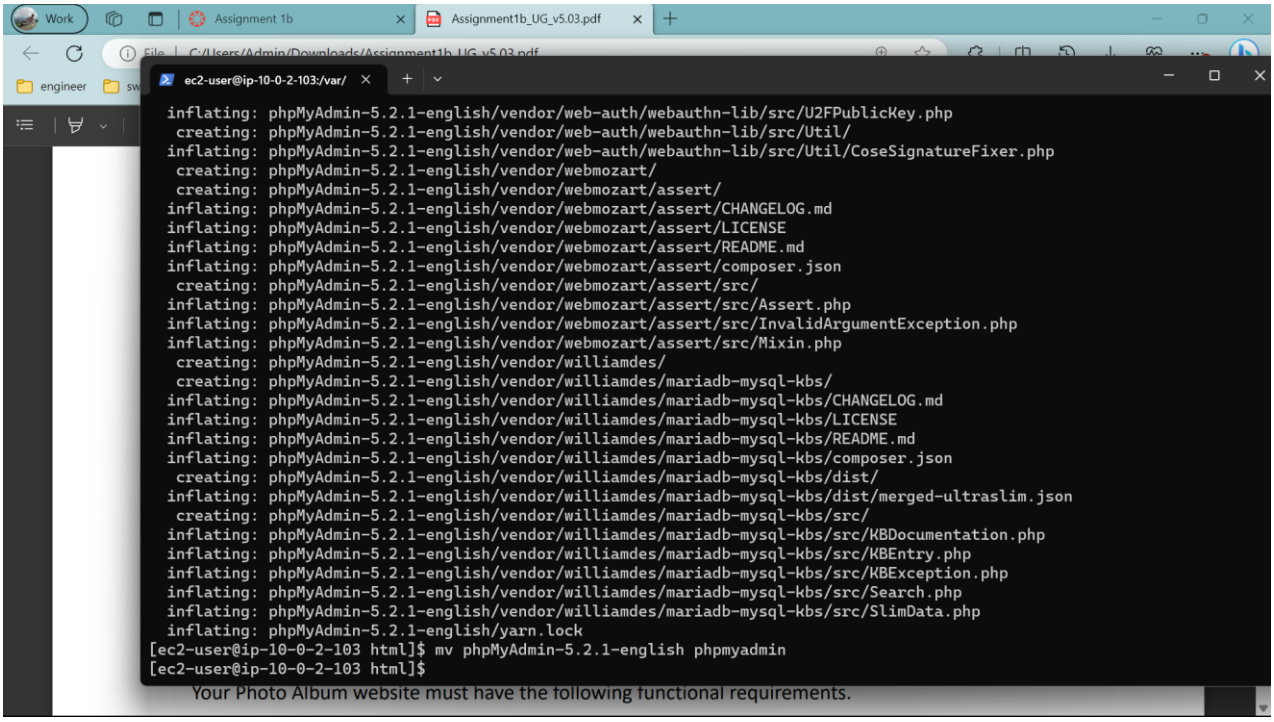

Figure 12: phpMyAdmin installed and moved on EC2 Instance

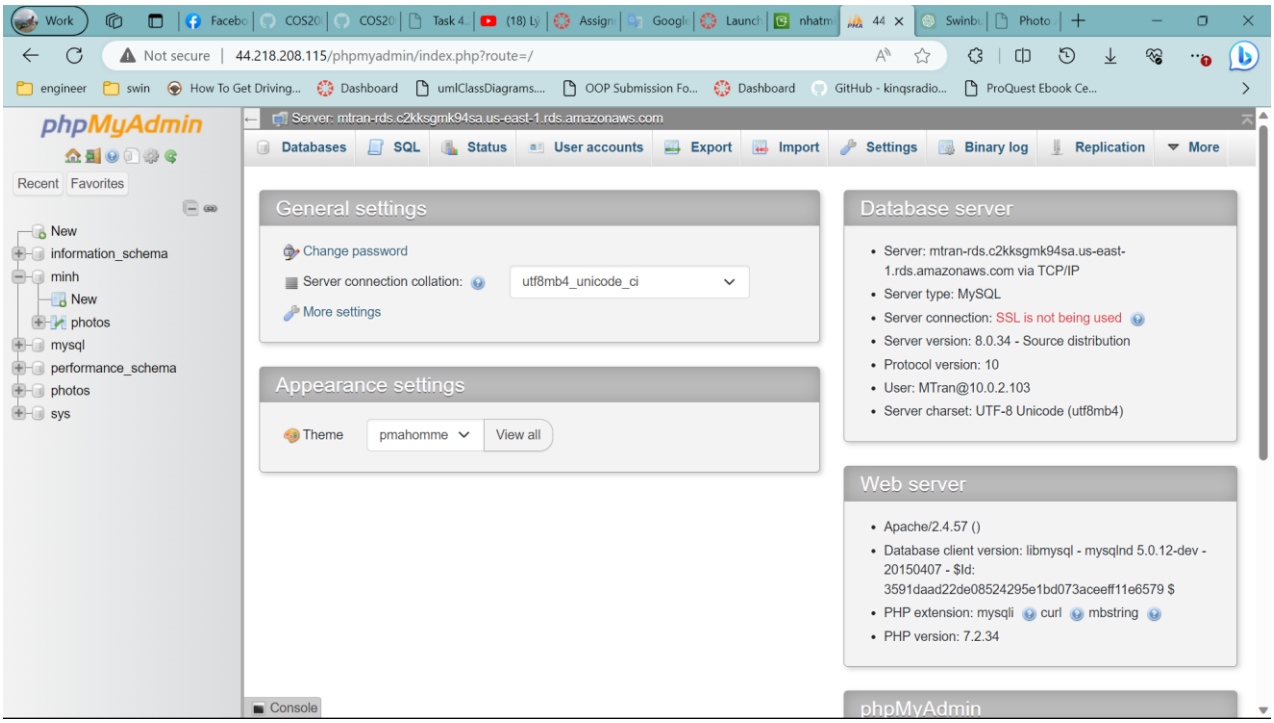

Figure 13: Webpage of phpMyAdmin

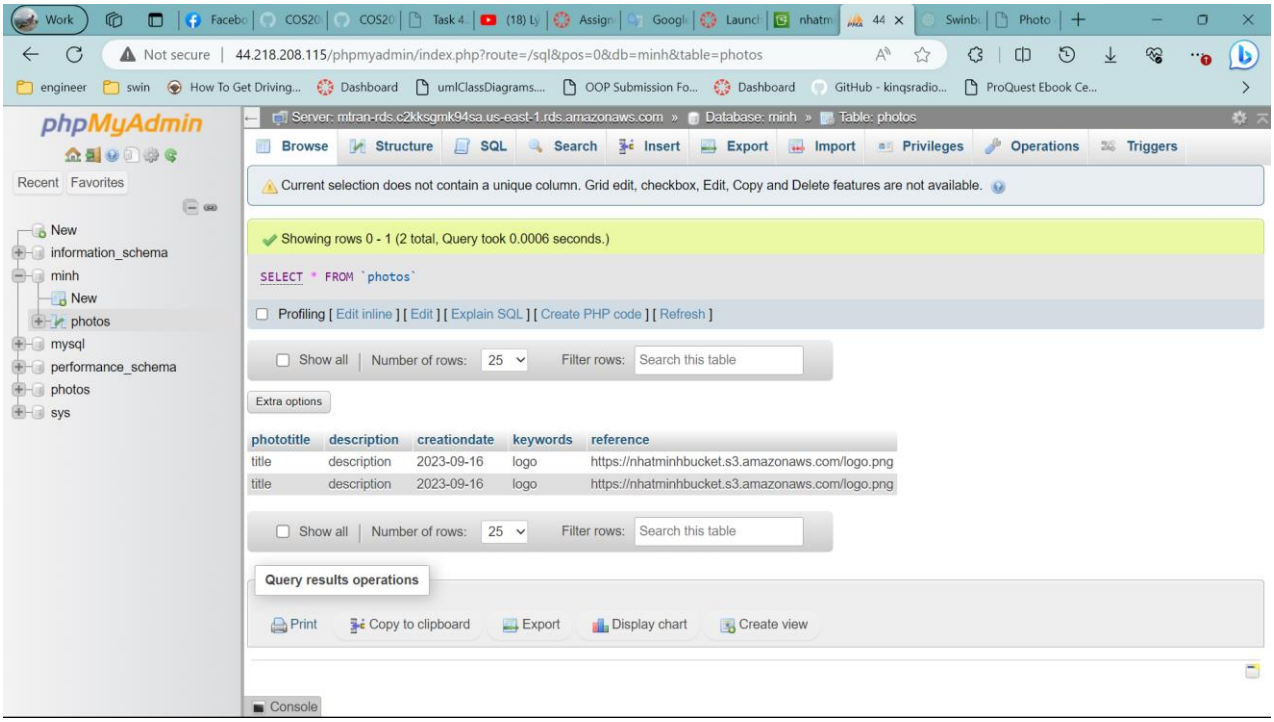

Figure 14: Table and data on webpage

1.5 – Network ACL

In AWS, NACL is a security layer that controls inbound and outbound traffic in the VPC. I have created a set of inbound and outbound rules to control the traffic coming into the subnet and the traffic leaving the subnet.

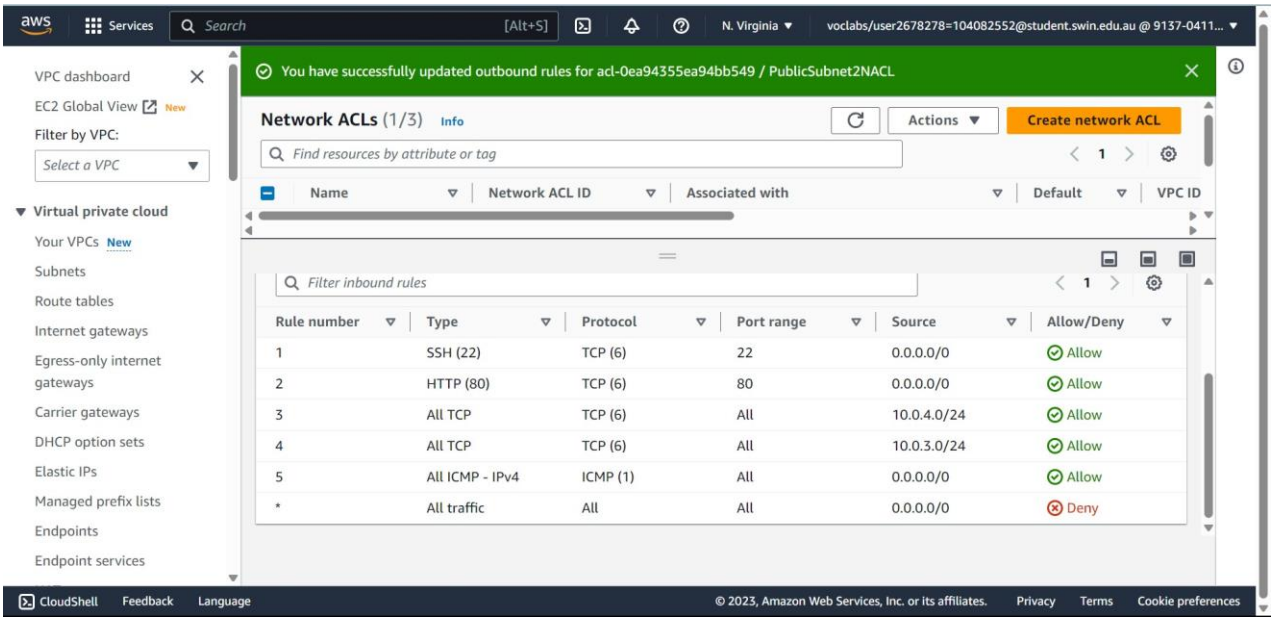

Figure 15: Inbound rules for NACL

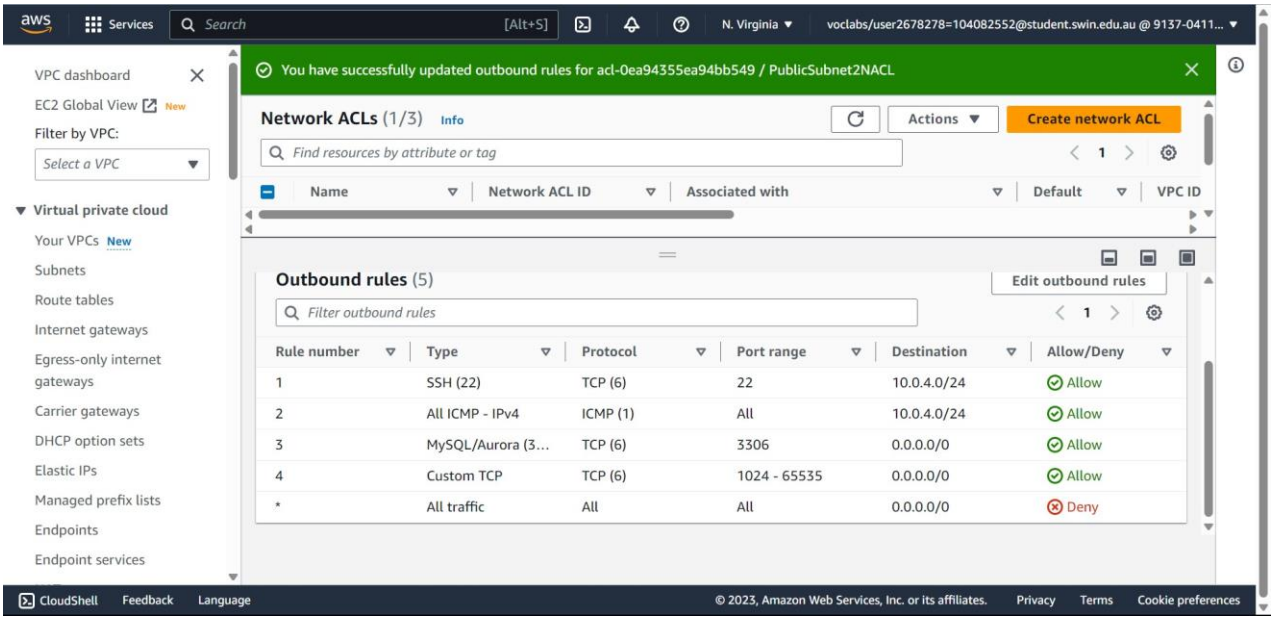

Figure 16: Outbound rules for NACL

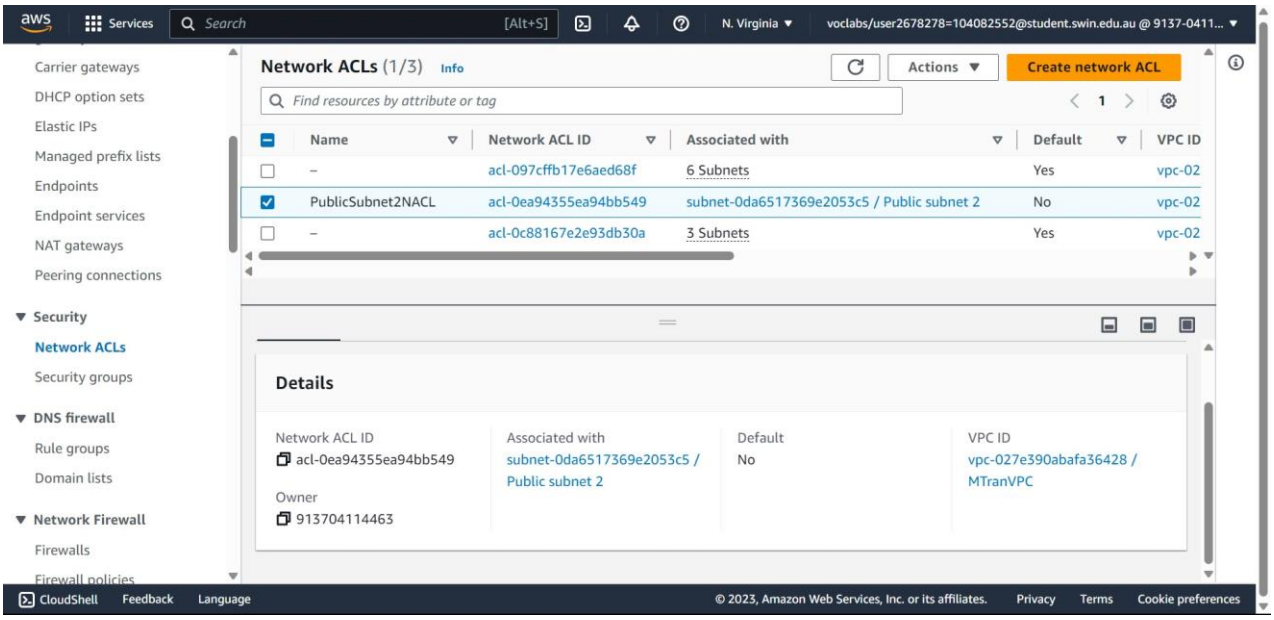

Figure 17: Network ACL is assigned to Public subnet 2

2. Functional requirements for Photo Album website

2.1 -Photo storage

S3 is a service that provided by AWS and allow you store and upload any photos, documents, videos… However, the photo that I uploaded cannot be seen right away, it needs bucket policy permissions to allow users to see it.

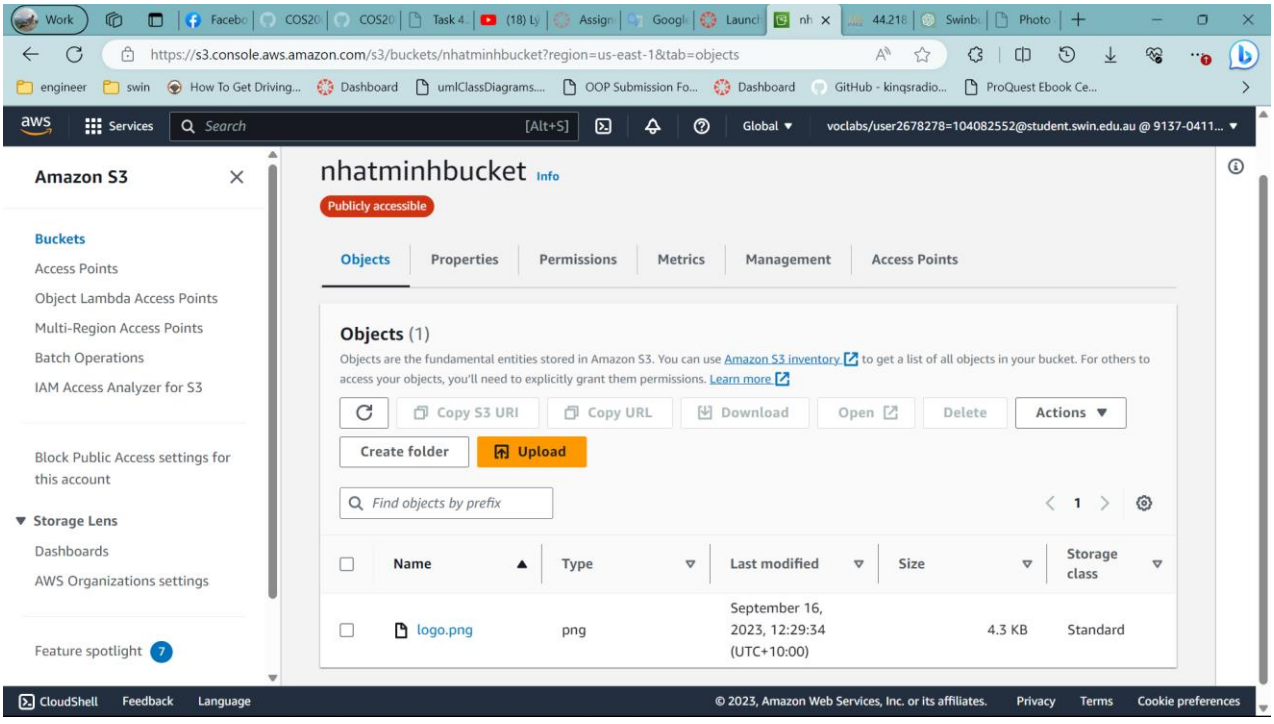

Figure 18: Nhatminhbucket

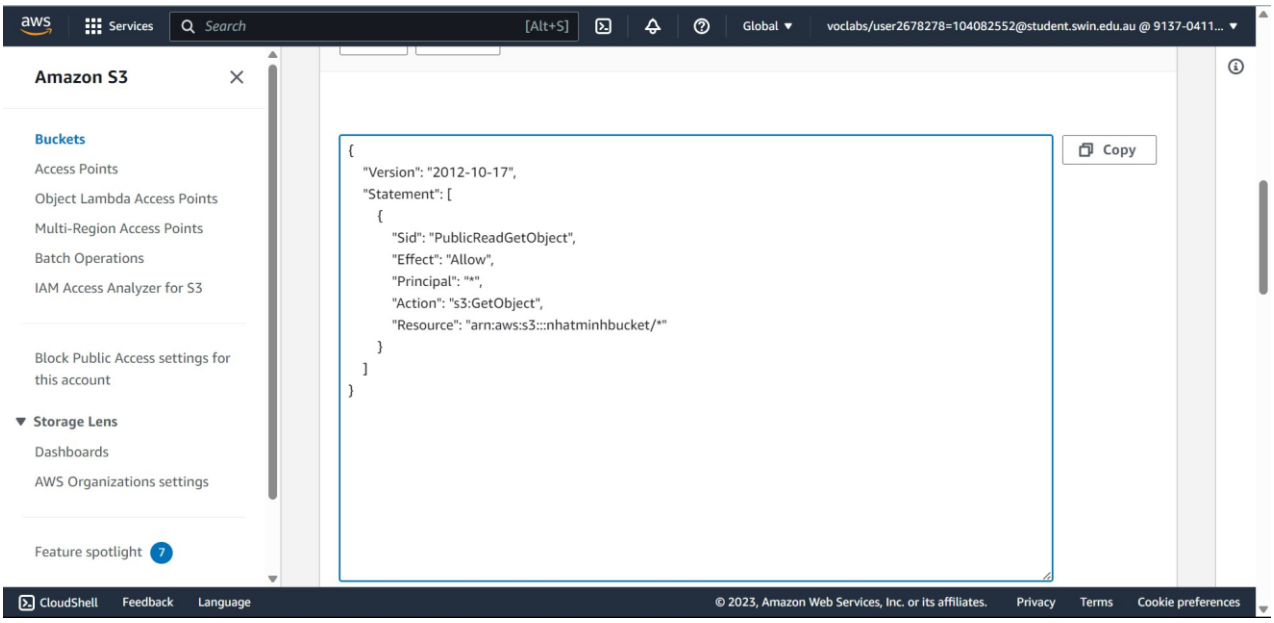

Figure 19: Policy permission for S3 bucket

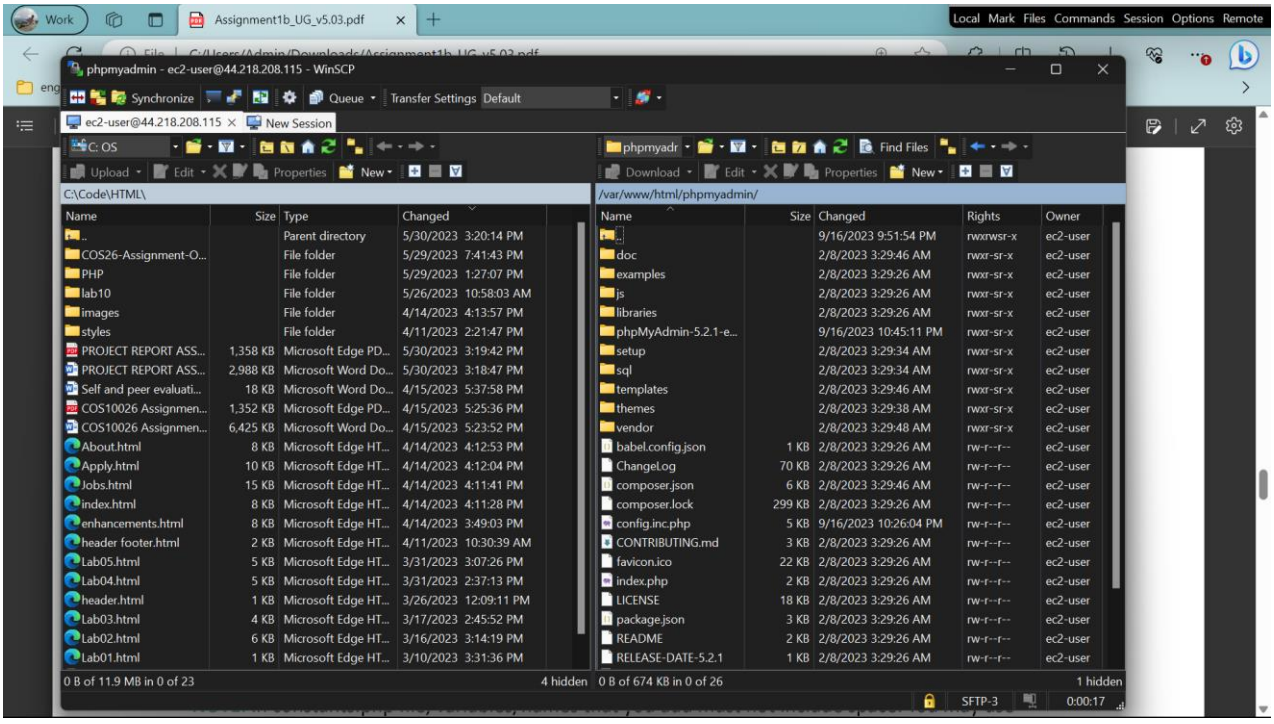

Figure 20: WinSCP connected with Minh.ppk authentication

2.2 – Photo meta-data in RDS instance

In this section, i created a table dedicated to photos, with five columns which are phototitle, description, creationdate, keywords, and reference. This data is used to display digital photos and videos on websites through phpMyAdmin service.

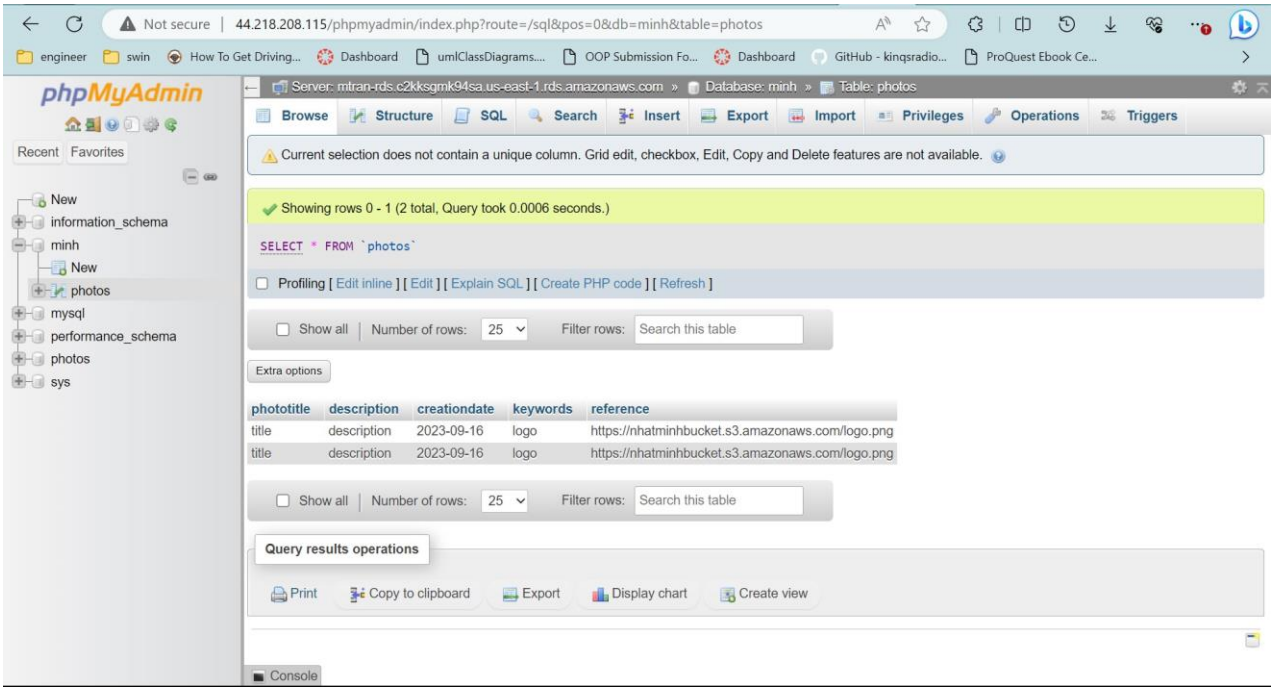

Figure 21: Meta-data of the website

2.3 – Photo Album website functionality

The website is completed with PHP, CSS, HTML files provided from school. In this stage, I have changed the constant.php to make it becomes website that unique to me such as student name, studentID, tutorial session, photos…

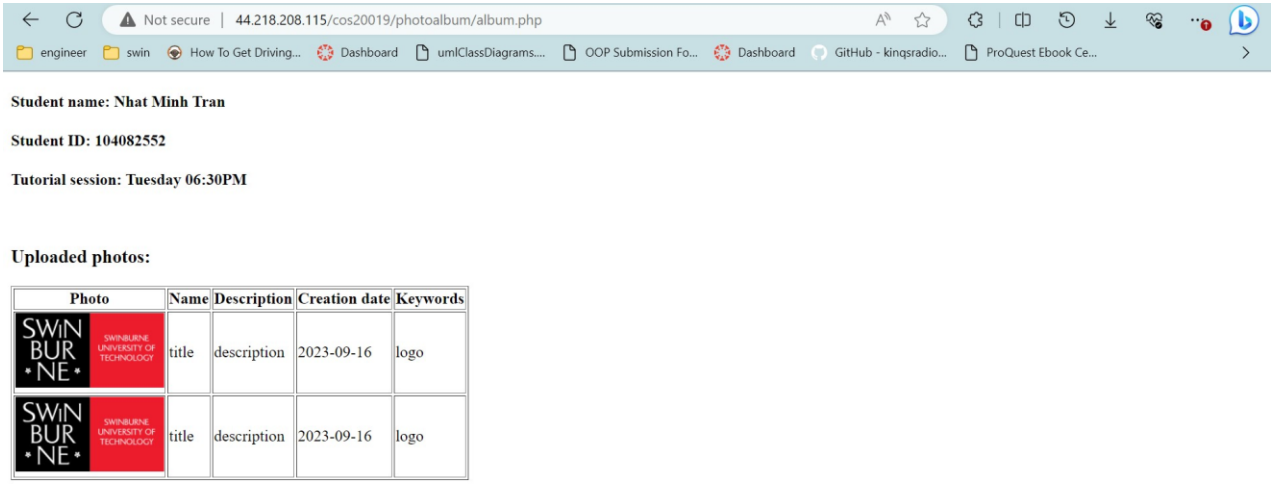

Figure 22: Functionality of the website

2.4 – Testing

To test our website and Network ACL configured correctly, the website can be ping between two IP.

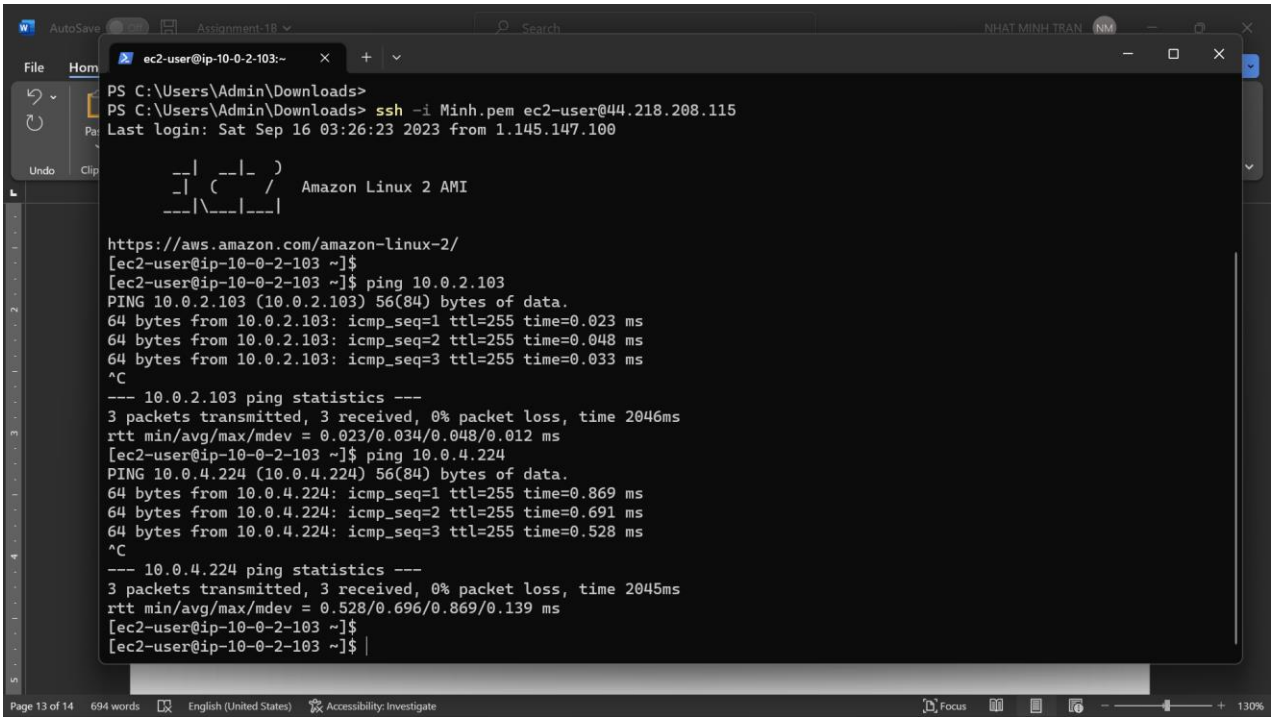

Figure 23: Ping between website successfully

Additional links for markings:

+ http://44.218.208.115/phpmyadmin
+ http://44.218.208.115/cos20019/photoalbum/album.php