**Axiom Assignment-1**

1. **Create a s3 bucket and limit access to particular user using Terraform.**

**Main.tf**

provider "aws"{

region ="us-west-2"

}

resource "aws\_s3\_bucket" "myBucket"{

bucket\_prefix= var.bucket\_prefix

acl = var.acl

tags= var.tags

}

resource "aws\_iam\_policy" "jsonencode"{

name = "tf-jsonencode"

policy = jsonencode({

"Version": "2012-10-17"

"Statement"= [

{

"Effect"= "Allow",

"Action"=[ "s3:ListBucket"],

"Resource"= [

aws\_s3\_bucket.myBucket.arn

]

},

{

"Effect"= "Allow",

"Action"=[ "s3:GetObject",

"s3:PutObject"

],

"Resource"= [

"${aws\_s3\_bucket.myBucket.arn}/\*"

]

}

]

})

}

**Variable.tf**

variable "bucket\_prefix"{

type = string

description = "Creates S3 bucket"

default = "my-s3-bucket-"

}

variable "tags"{

type = map

default={

terraform = true,

environment = "DEV"

}

}

variable "acl"{

type = string

default = "private"

}

JSON CODE for policy which is edit on AWS Console.

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Deny",

"Action": "s3:ListBucket",

"Resource": "arn:aws:s3:::my-s3-bucket-20220104135826514400000001",

"Condition": {

"StringNotLike": {

"aws:userName": [

"eswar"

]

}

}

},

{

"Sid": "VisualEditor1",

"Effect": "Deny",

"Action": "s3:ListAllMyBuckets",

"Resource": "\*",

"Condition": {

"StringNotLike": {

"aws:userName": [

"eswar"

]

}

}

},

{

"Sid": "VisualEditor2",

"Effect": "Deny",

"Action": [

"s3:PutObject",

"s3:GetObject"

],

"Resource": "arn:aws:s3:::my-s3-bucket-20220104135826514400000001/\*",

"Condition": {

"StringNotLike": {

"aws:userName": [

"eswar"

]

}

}

},

{

"Sid": "VisualEditor3",

"Effect": "Deny",

"Action": "s3:ListBucket",

"Resource": "arn:aws:s3:::my-s3-bucket-20220104135826514400000001"

},

{

"Sid": "VisualEditor4",

"Effect": "Allow",

"Action": "s3:ListAllMyBuckets",

"Resource": "\*"

},

{

"Sid": "VisualEditor5",

"Effect": "Allow",

"Action": [

"s3:PutObject",

"s3:GetObject"

],

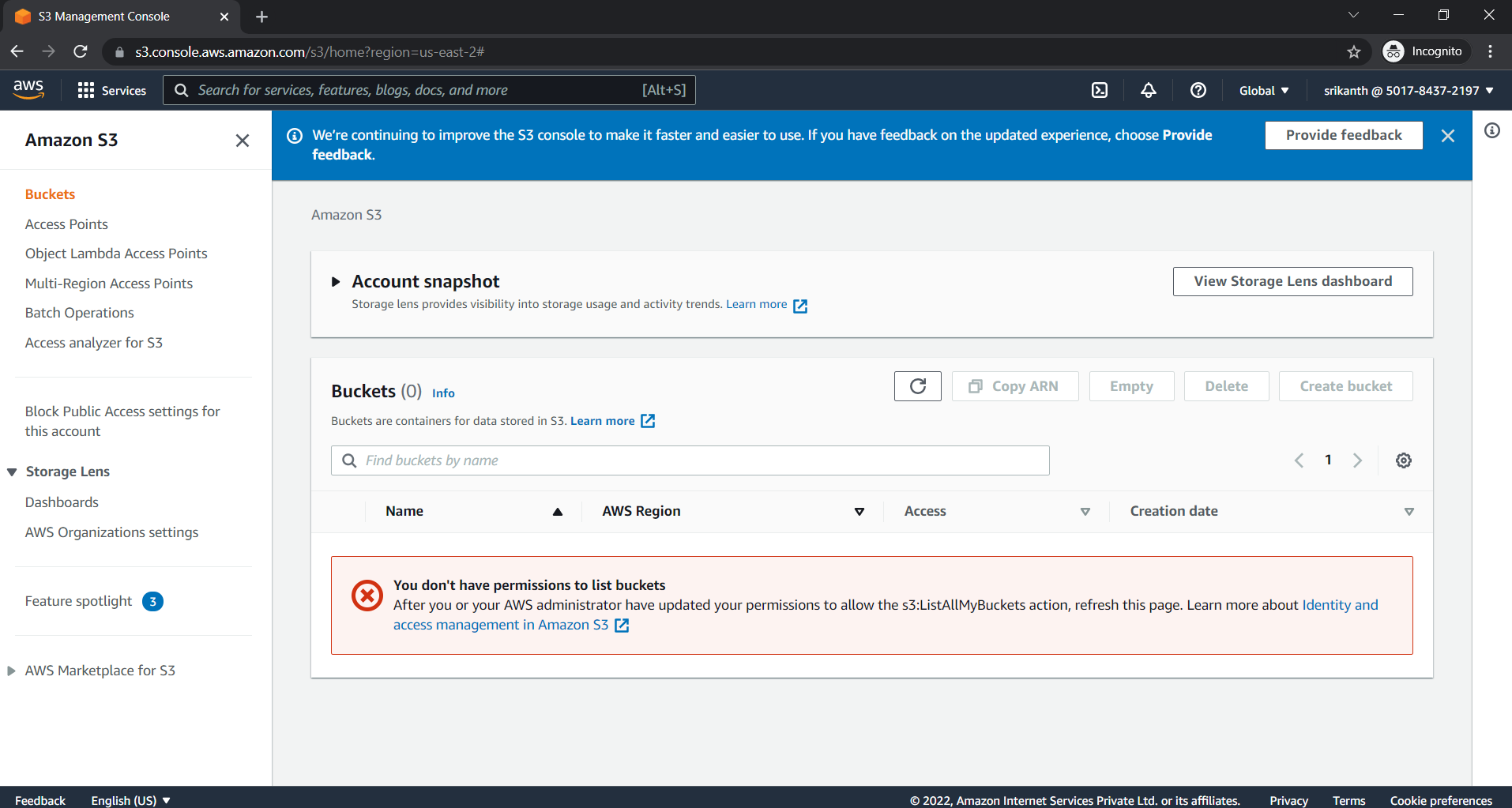
"Resource": "arn:aws:s3:::my-s3-bucket-20220104135826514400000001/\*"

}

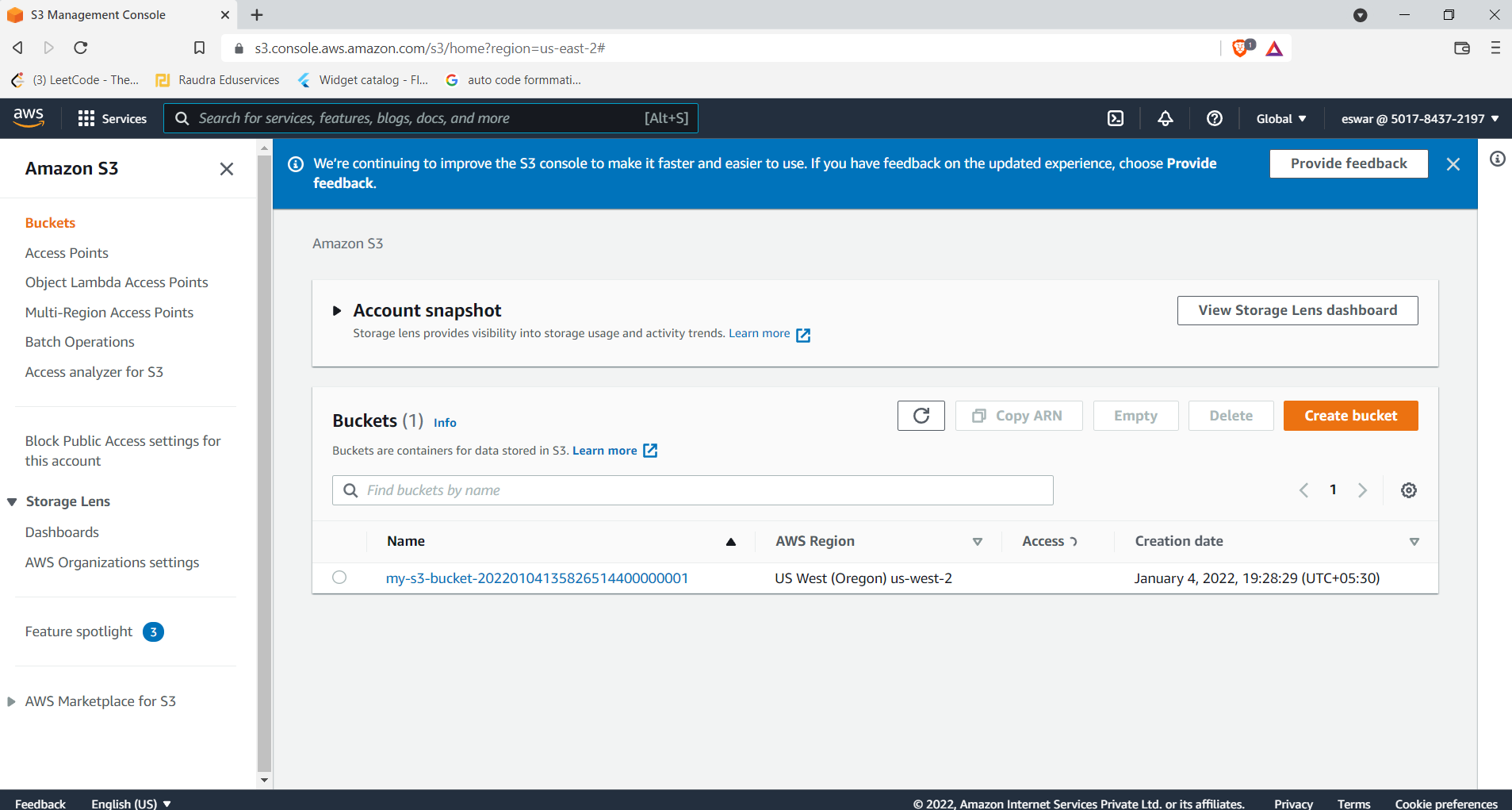
]

}

User srikanth console :(Whom I restricted)



User eswar console :

****

**2.Modules for vpc,subnets,natgateways,internetgateway,**

**ec2 .**

**.**Module Folder contains these files

main.tf

terraform {

required\_version = ">= 0.12"

}

resource "aws\_subnet" "webserver"{

vpc\_id = var.vpc\_id

cidr\_block = var.cidr\_block

}

resource "aws\_instance" "server"{

ami = var.ami

instance\_type = var.instance\_type

subnet\_id = aws\_subnet.webserver.id

tags={

Name ="${var.webserver\_name} Webserver"

}

}

resource "aws\_eip" "lb" {

instance = aws\_instance.server.id

vpc = true

}

resource "aws\_nat\_gateway" "gw" {

allocation\_id = aws\_eip.lb.id

subnet\_id = aws\_subnet.webserver.id

}

resource "aws\_internet\_gateway" "gw" {

vpc\_id = var.vpc\_id

}

variable "vpc\_id"{

type =string

description = "VPC id"

default="my-s3-bucket-"

}

variable "cidr\_block"{

type = string

description ="subnet cidr\_block"

}

variable "webserver\_name"{

type=string

description ="webserver name"

}

variable "ami"{

type = string

description = "AMI to use foe webserver"

}

variable "instance\_type"{

type = string

description = "instance type"

}

The other folder which is setup contains the following main file

main.tf

provider "aws"{

region = "us-west-1"

}

resource "aws\_vpc" "myVpc"{

cidr\_block = "10.0.0.0/16"

}

module "chandra\_webserver"{

source = "../modules/webserver"

vpc\_id = aws\_vpc.myVpc.id

cidr\_block = "10.0.0.0/16"

webserver\_name = "chandra"

ami = "ami-03af6a70ccd8cb578"

instance\_type="t2.micro"

}

