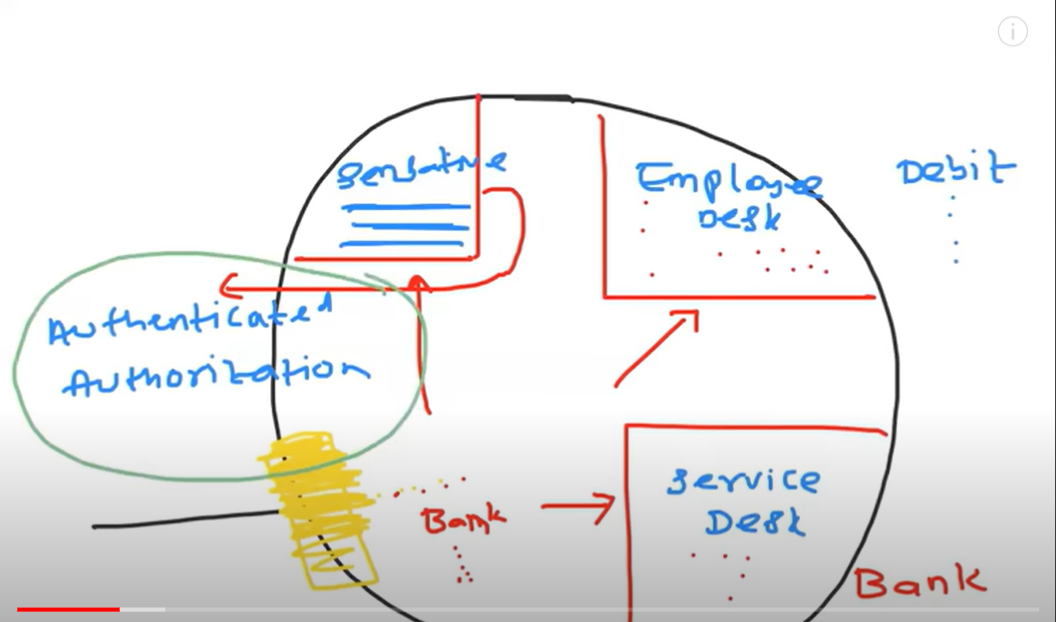
AWS IAM SERVICE

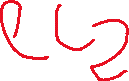


Let's imagine a scenario where there is a bank with two distinct areas. The first area is sensitive and holds crucial documents and files, while the second area has an employee desk for addressing customer queries related to debit and credit cards. There is also a service desk that provides customer service. To enter the bank, you need to be an authenticated user, meaning you must have an account with the bank. We will then check your authentication to confirm that you are an account holder, a superior authority, or an employee. The bank has set up dedicated authenticated authorization. If proper authentication and authorization measures are not implemented, unauthorized individuals could easily gain access to the bank and steal money, making these measures crucial.

Try to convert this example in terms of AWS

Let’s say you have created an AWS account for your organization. As a DevOps Engineer, you need to create an AWS account for Example.com.

Example.com



Let’s assume, there is no authentication service is not there in AWS. Then root user privileges are granted to all people. And they might knowingly or unknowingly delete that data or edit or update the data…it becomes very hectic for the organization.

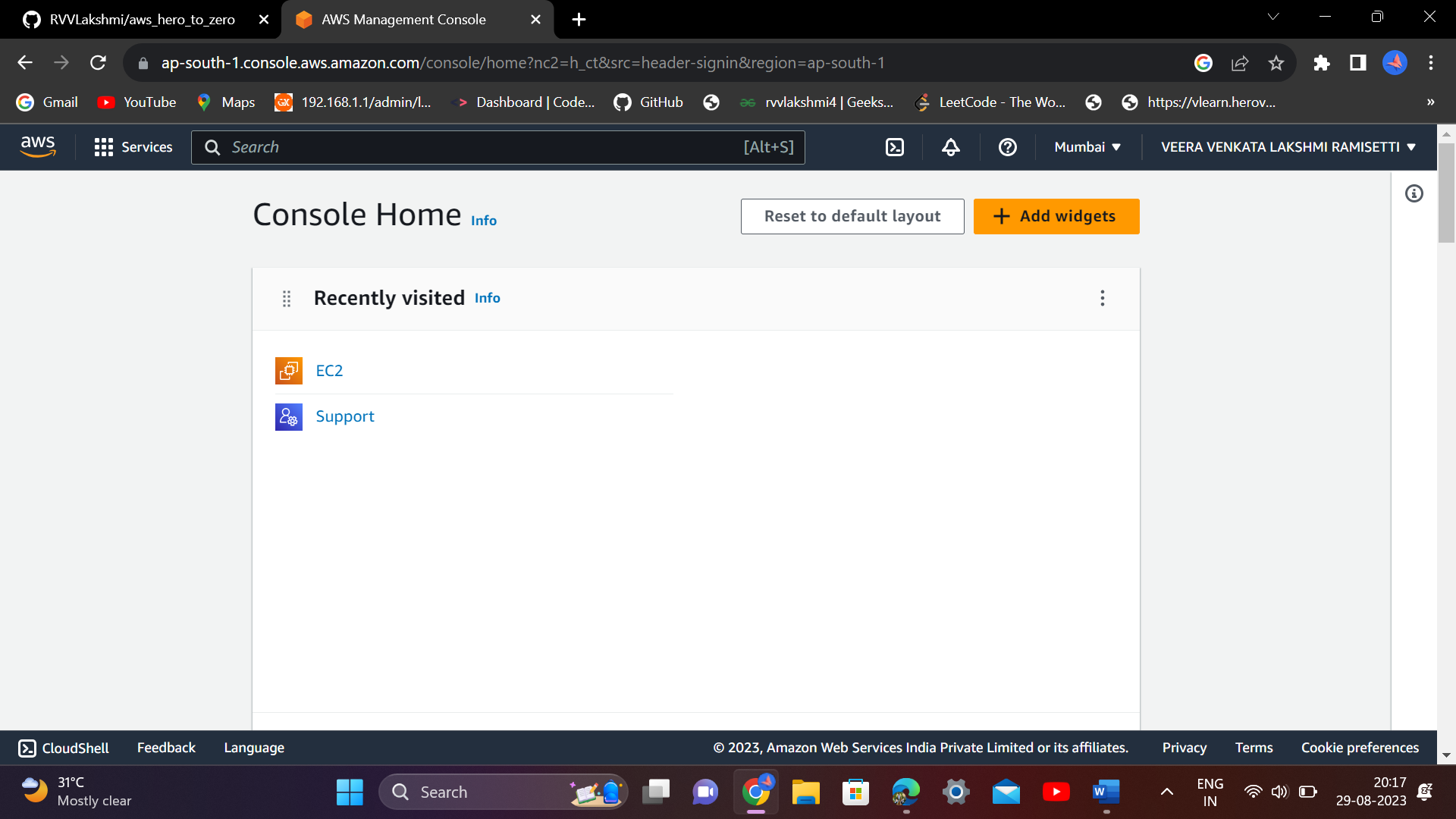
AWS Identity and Access Management (IAM)

IAM in AWS is a service that does authentication and authorization.

Let’s say user 501 has joined in your organization Example.com recently. He requested you to create an AWS account for him. As a DevOps engineer, you need to create an account but you had asked him like this, I would create an account for you, but let me know what services you want access.

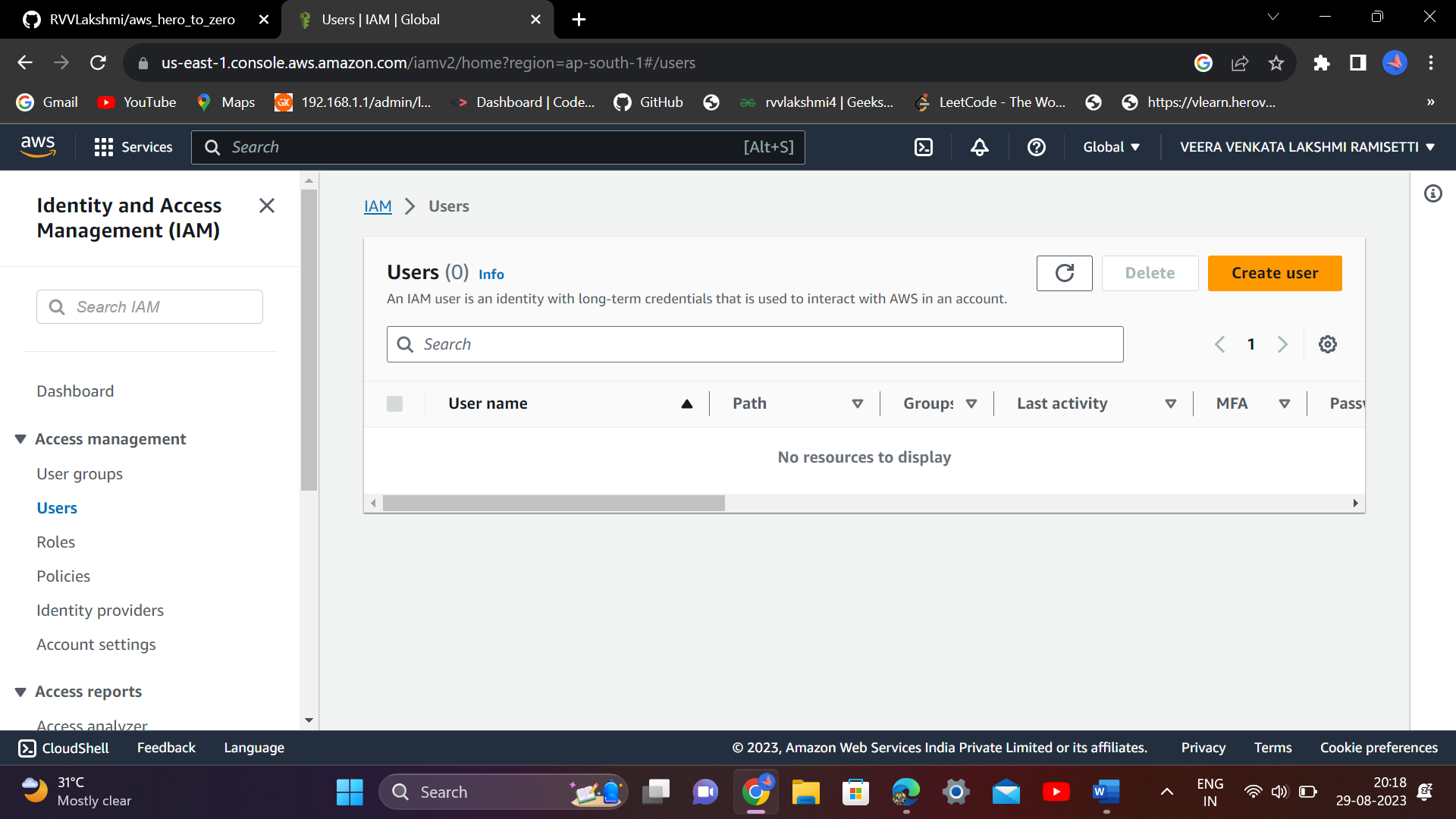
LAB

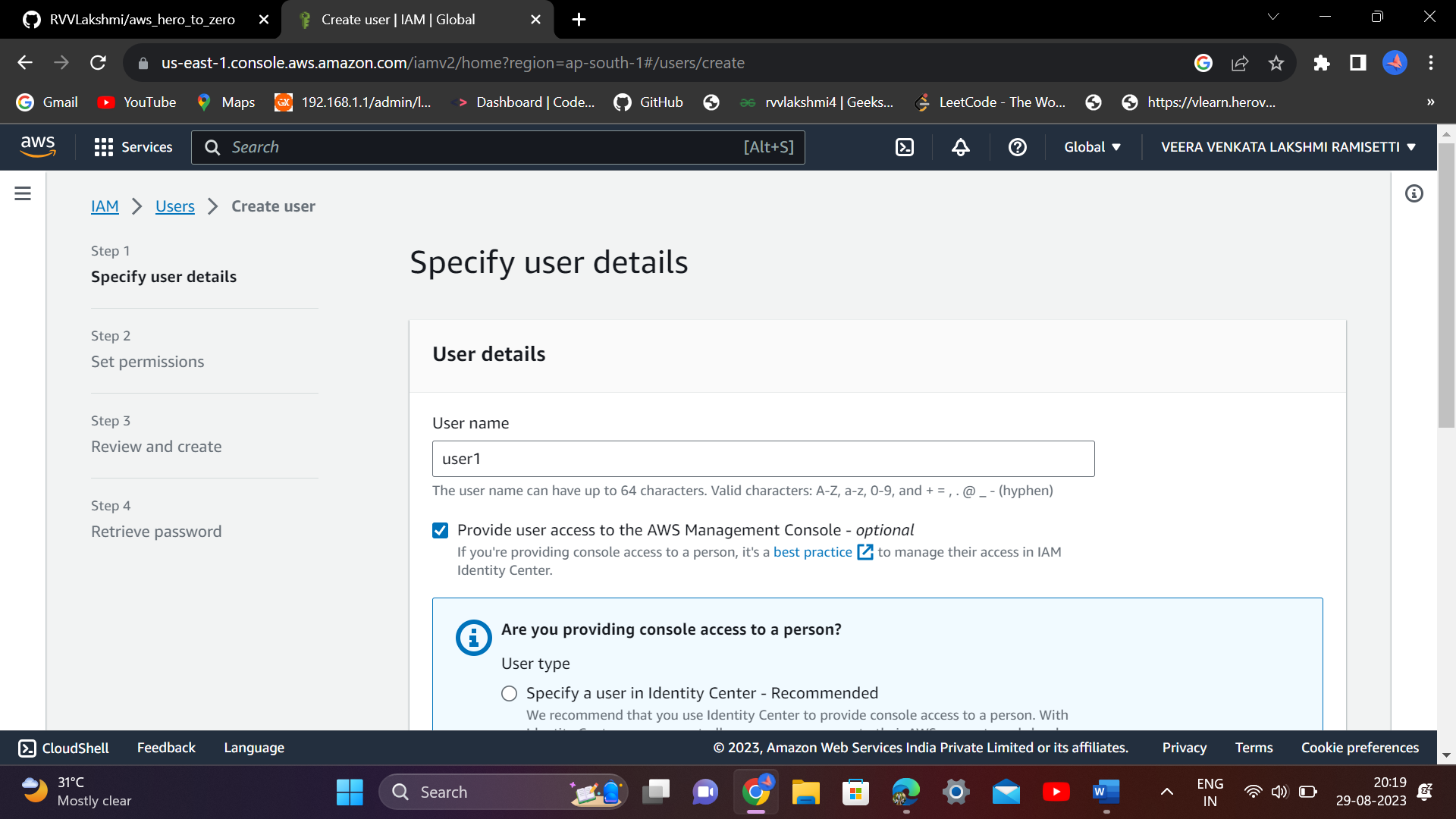
First login into account



Then search for IAM service

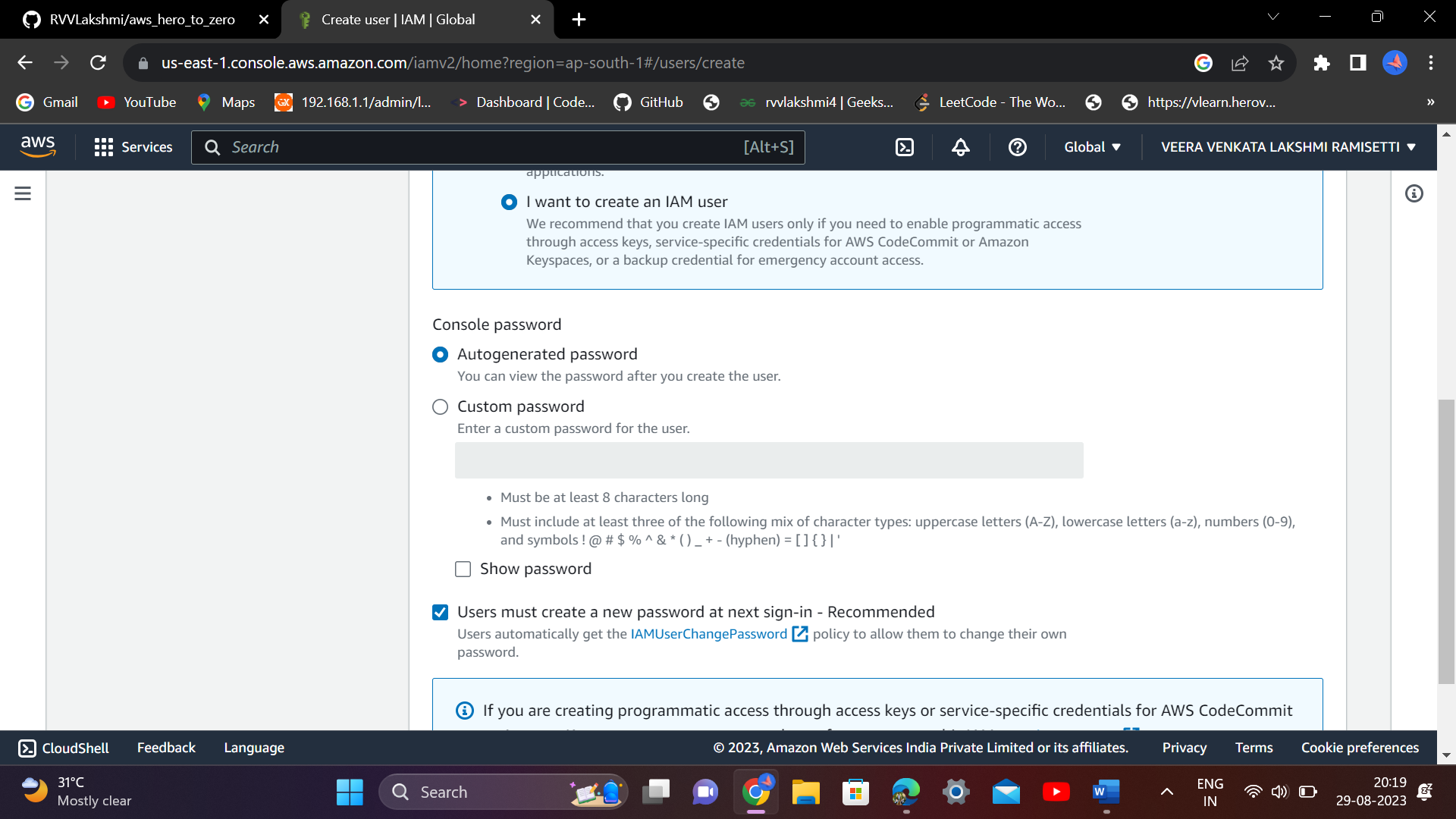
Let’s first create an user

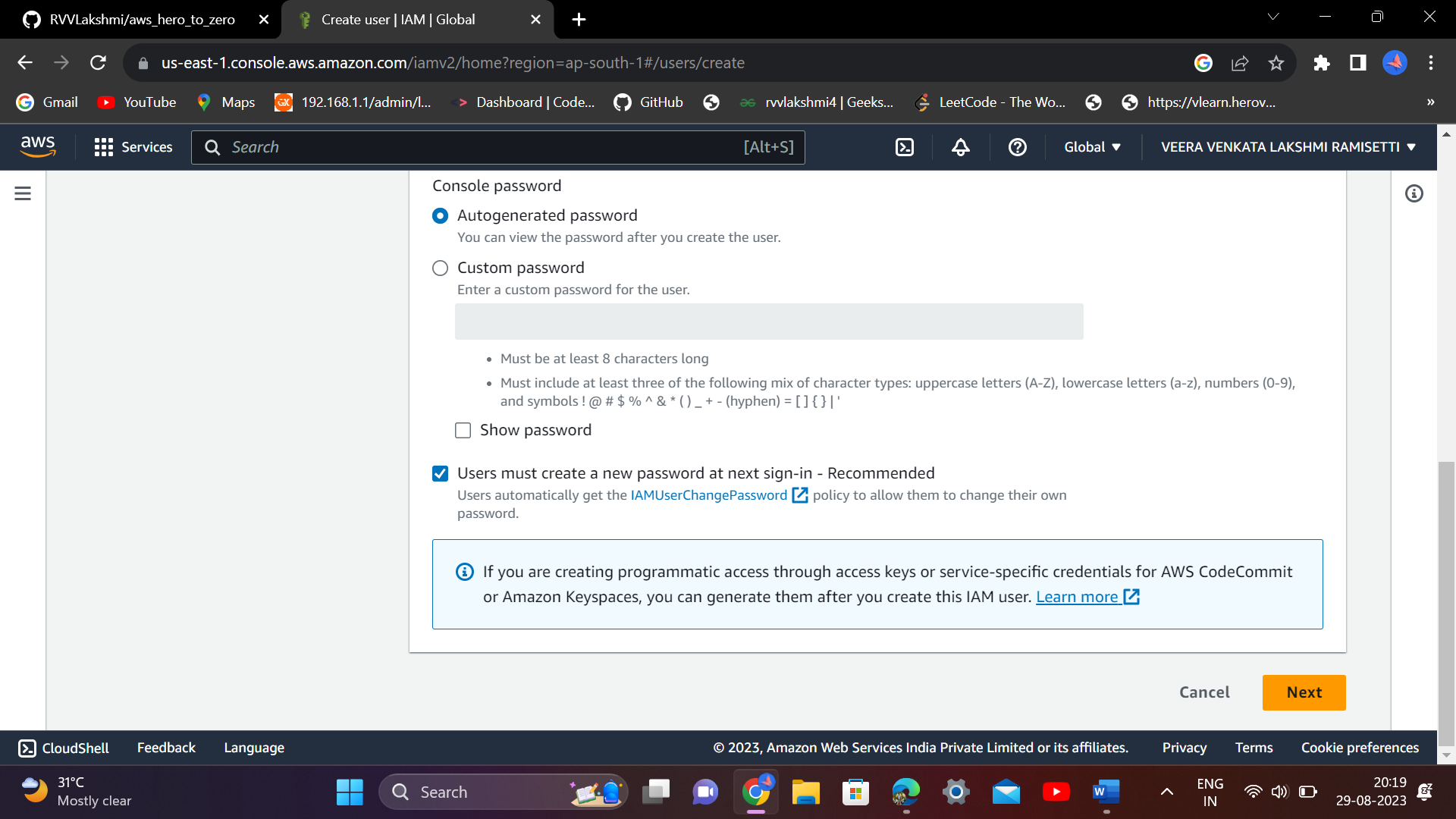




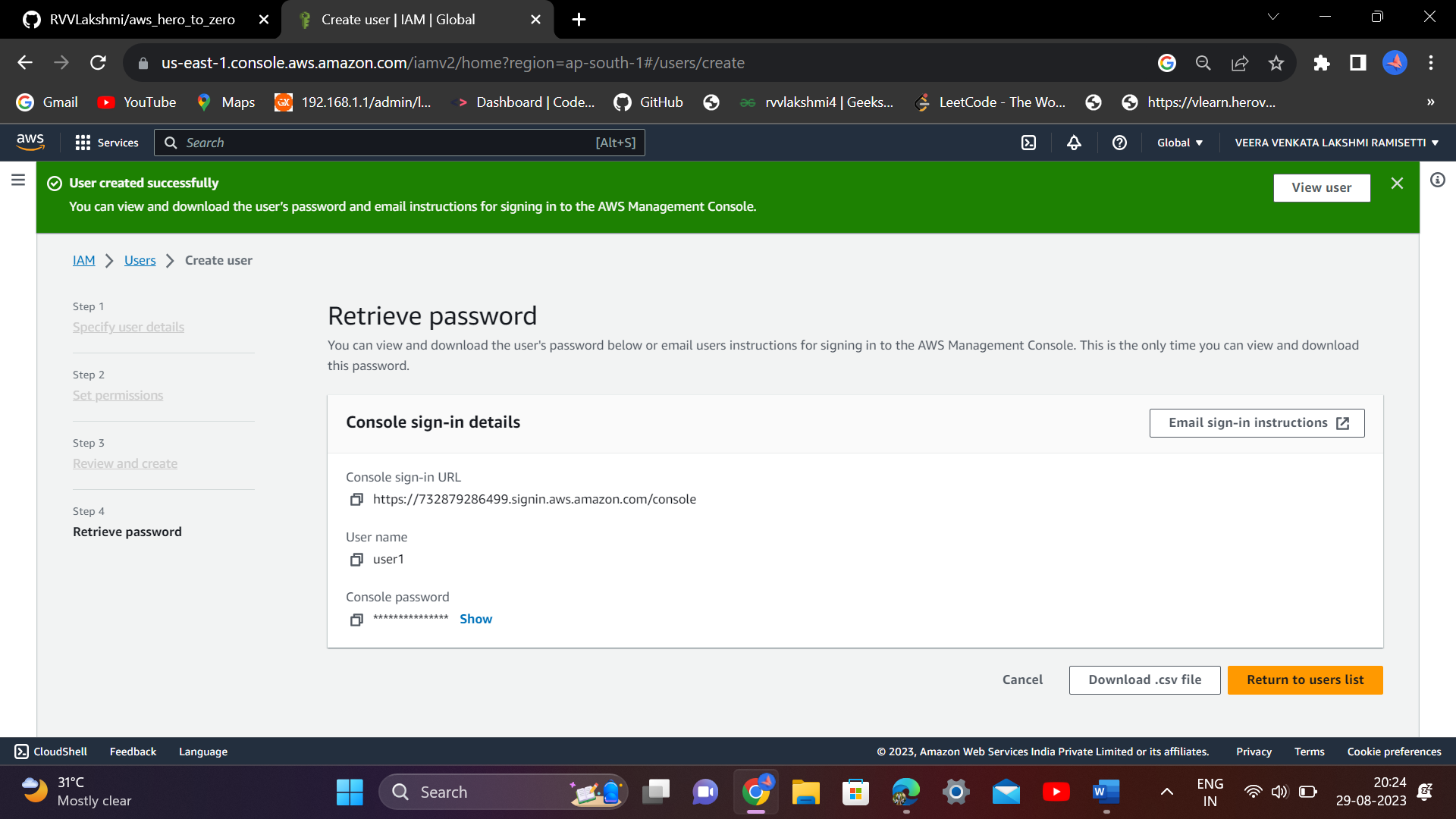
**Create an IAM user(not a root user)**

**An autogenerated password means you don’t need to generate a password for the creating users every time…An automatic pass will come.**

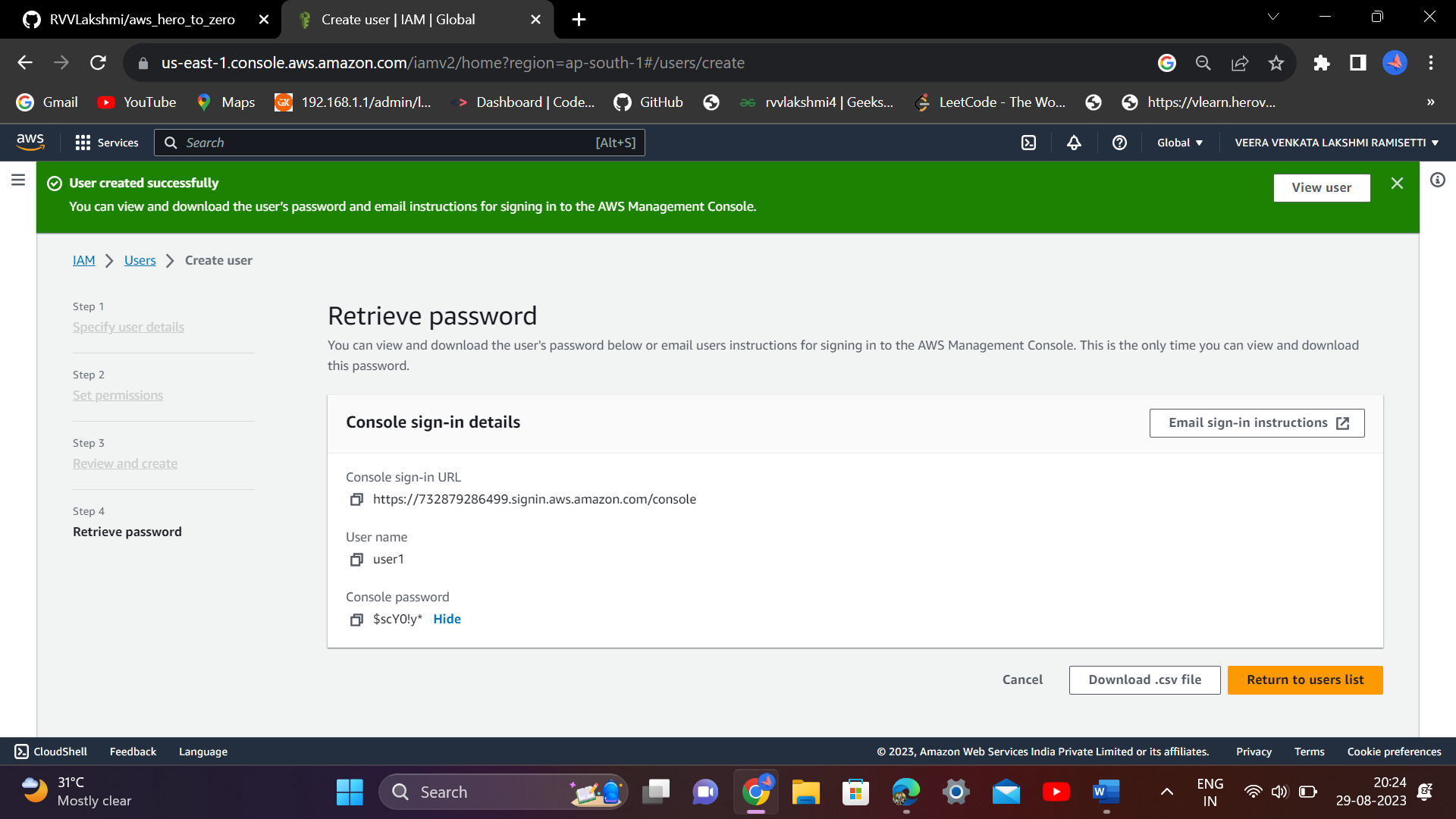


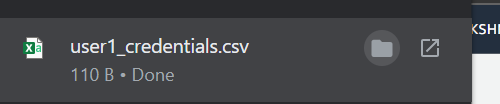


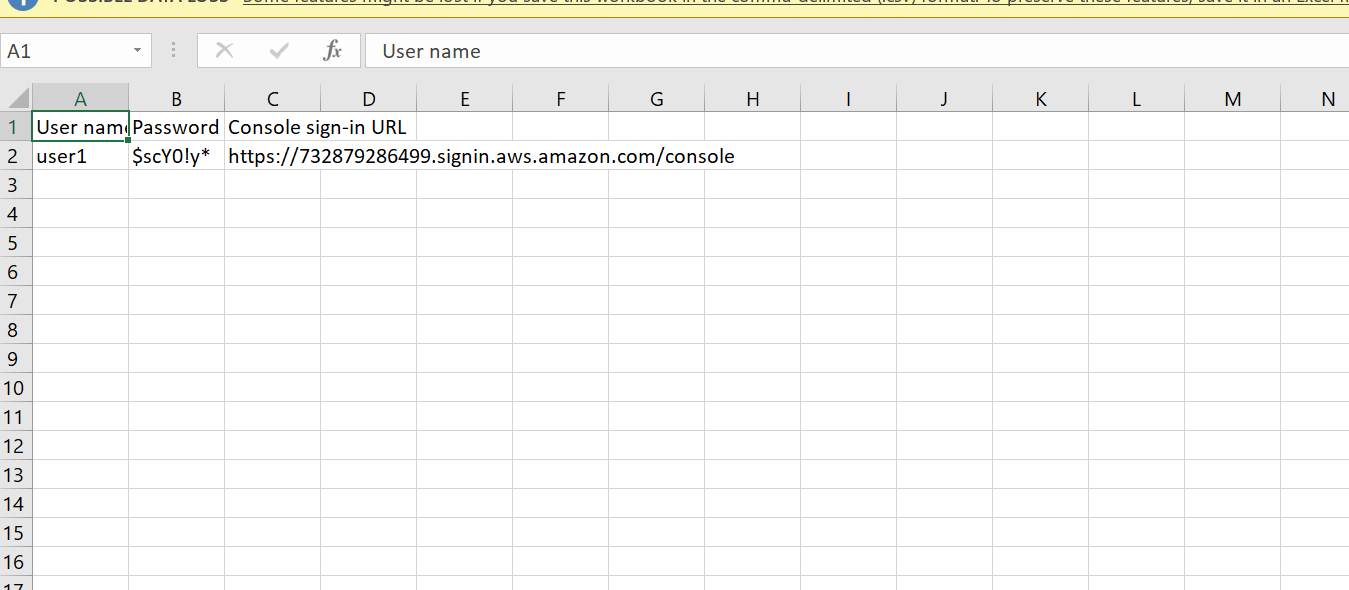




Download the .csv file for future reference



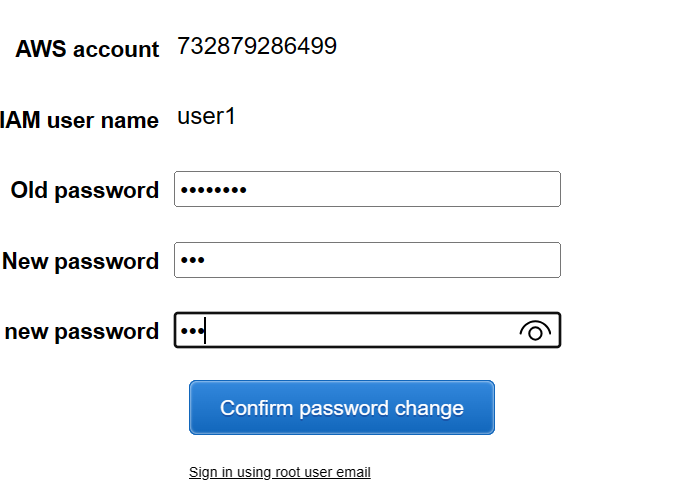




Sign in using these credentials

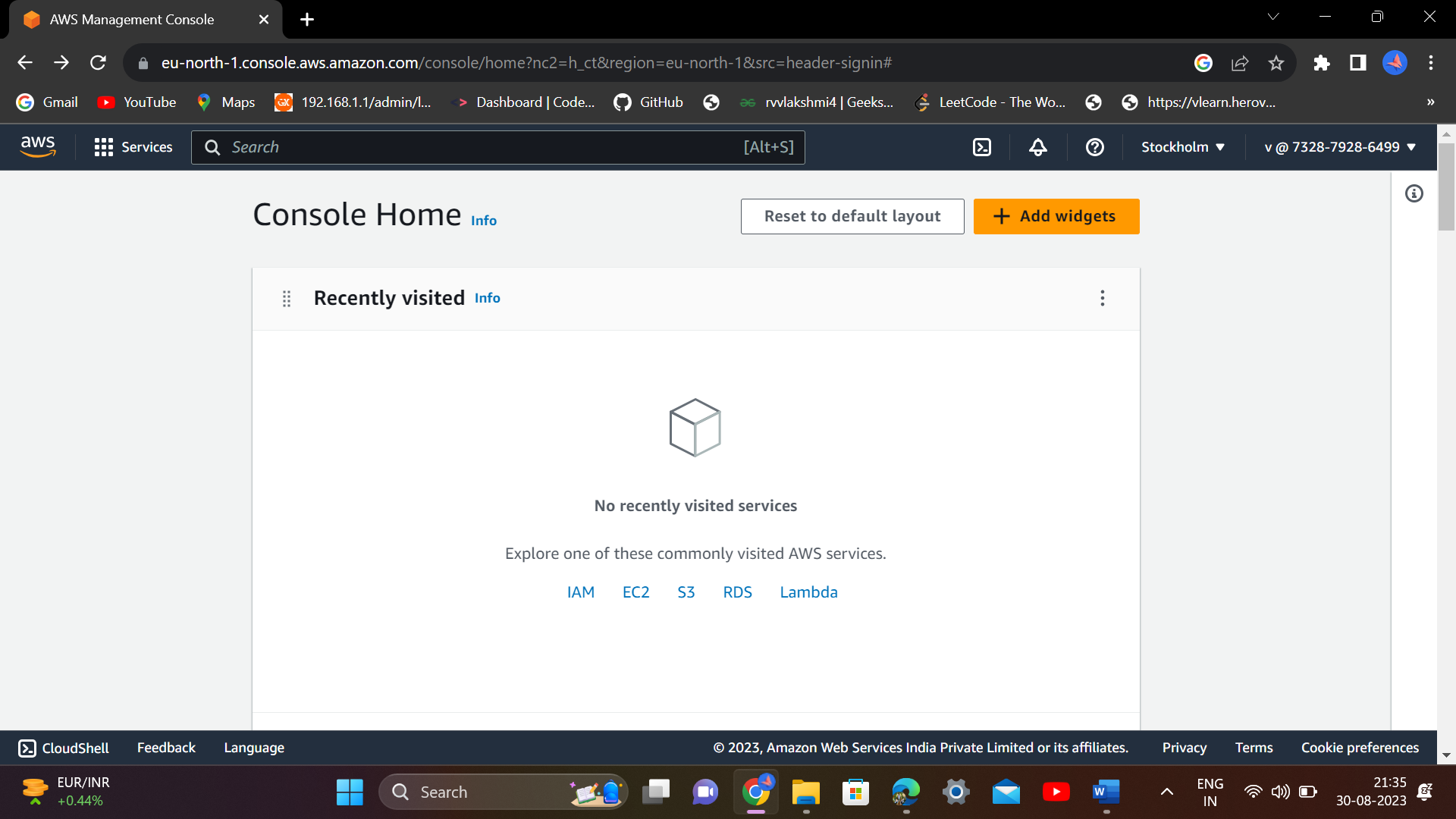
732879286499 as account id (12 digits)



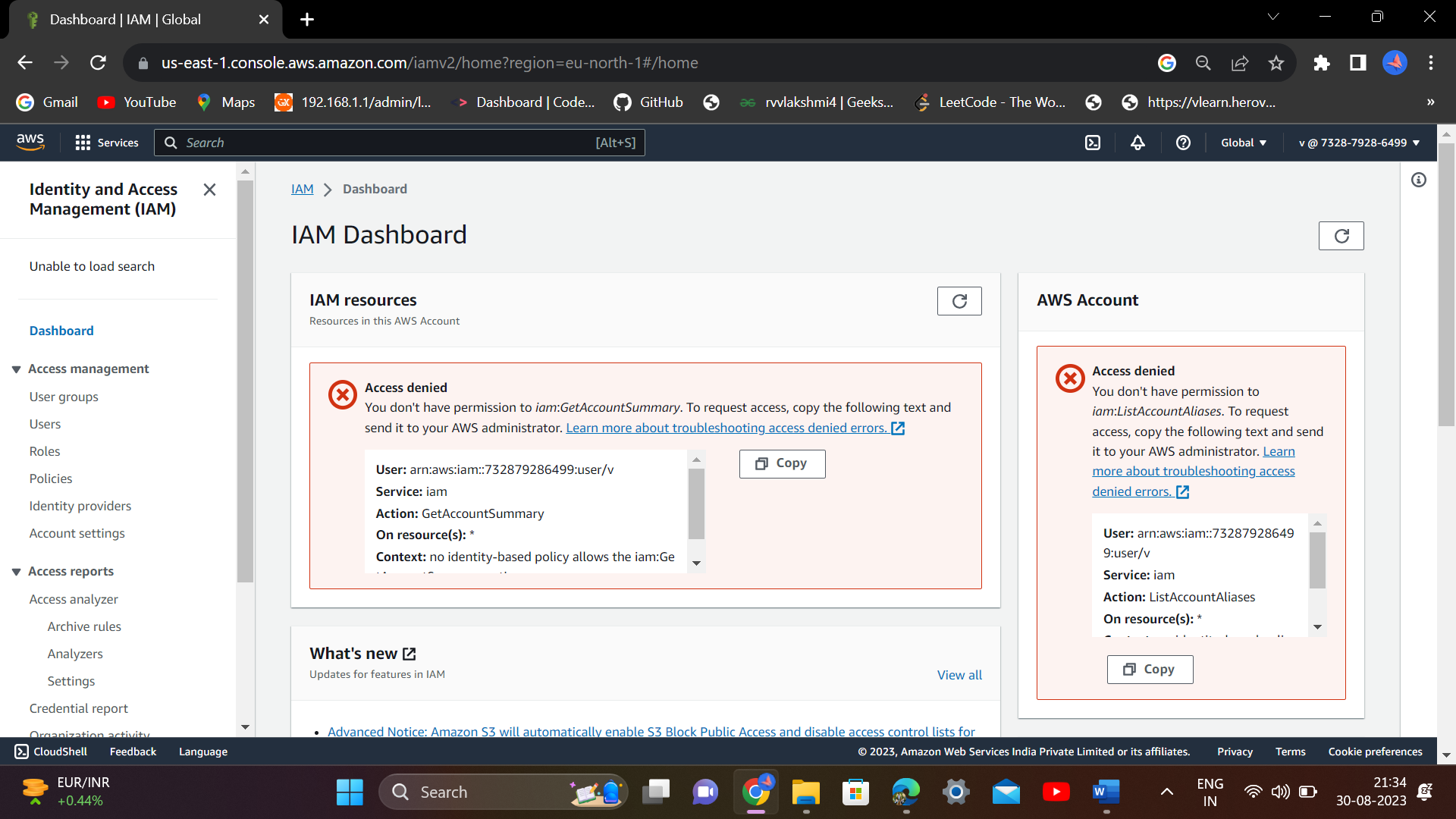


Minimum password length of 8 characters and a maximum length of 128 characters. Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and non-alphanumeric character ( ! @ # $ % ^ & \* ( ) \_ + - = [ ] { } | ' ) Not be identical to your AWS account name or email address.

After login:

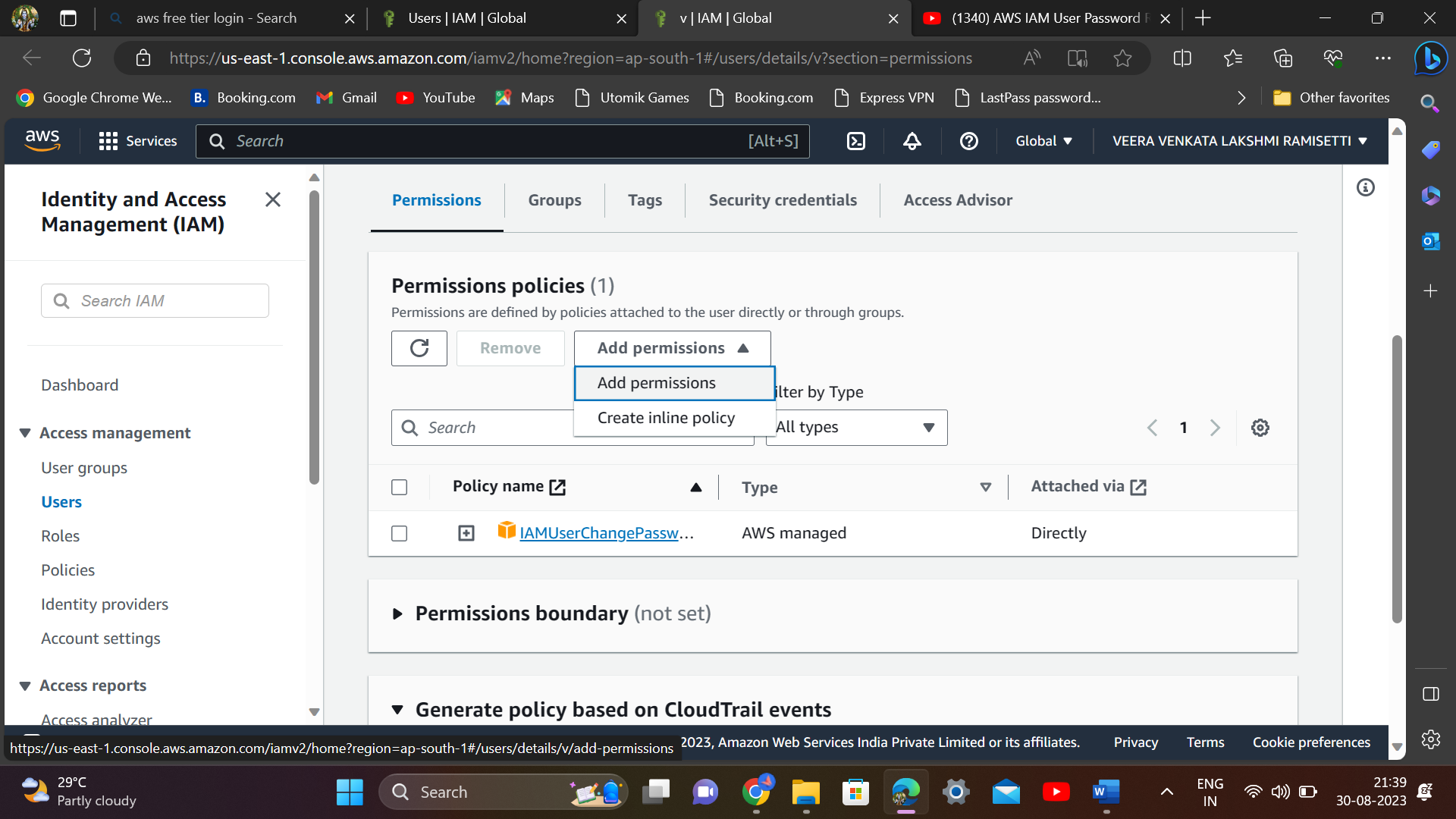


Still u don’t have permissions use this services..if you want to use any services you have to request admin(root user) DevOps engineer.

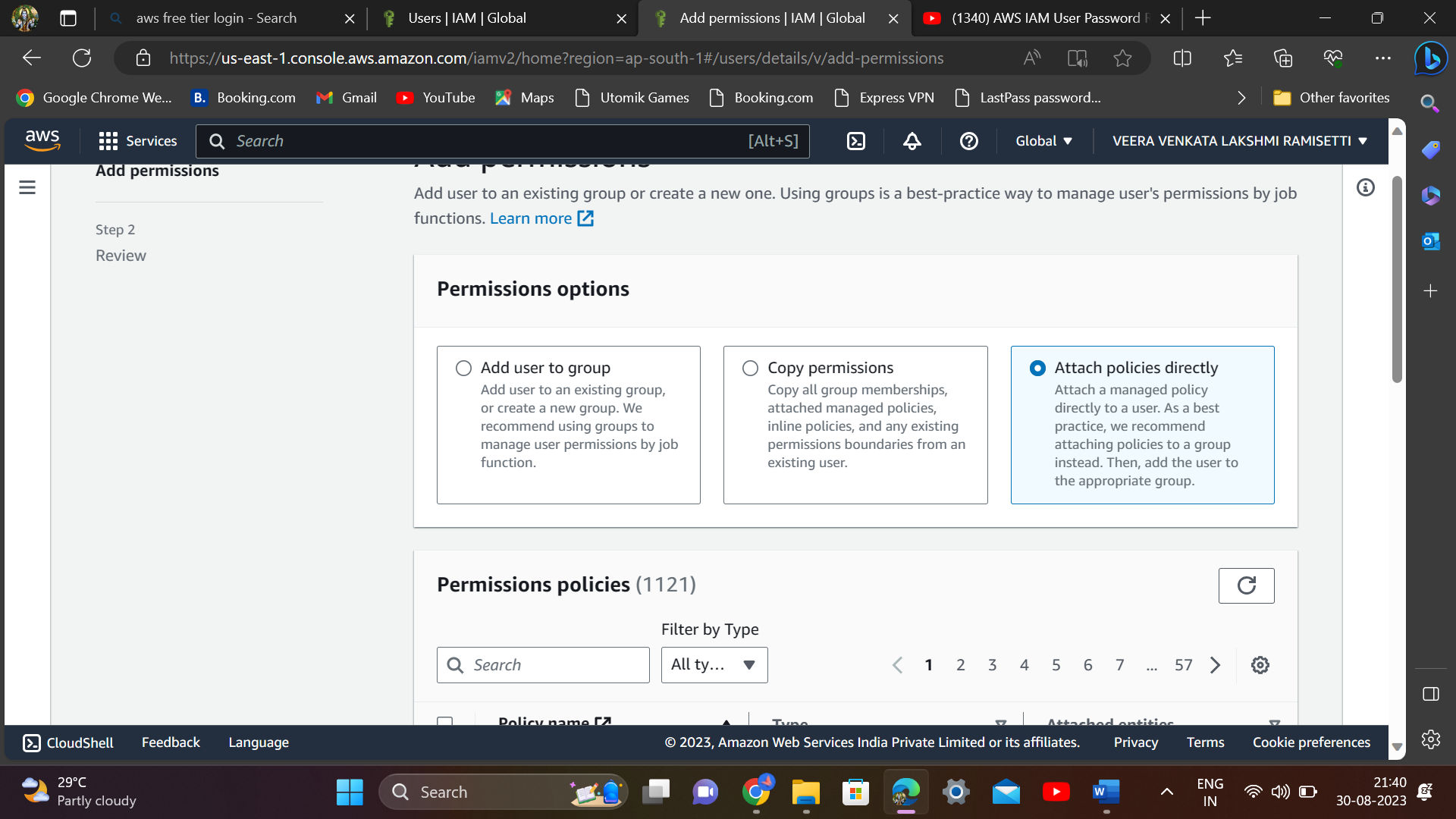


After requesting I am user, if you are a DevOps engineer...u need to follow this process

U need to add permissions for this particular user

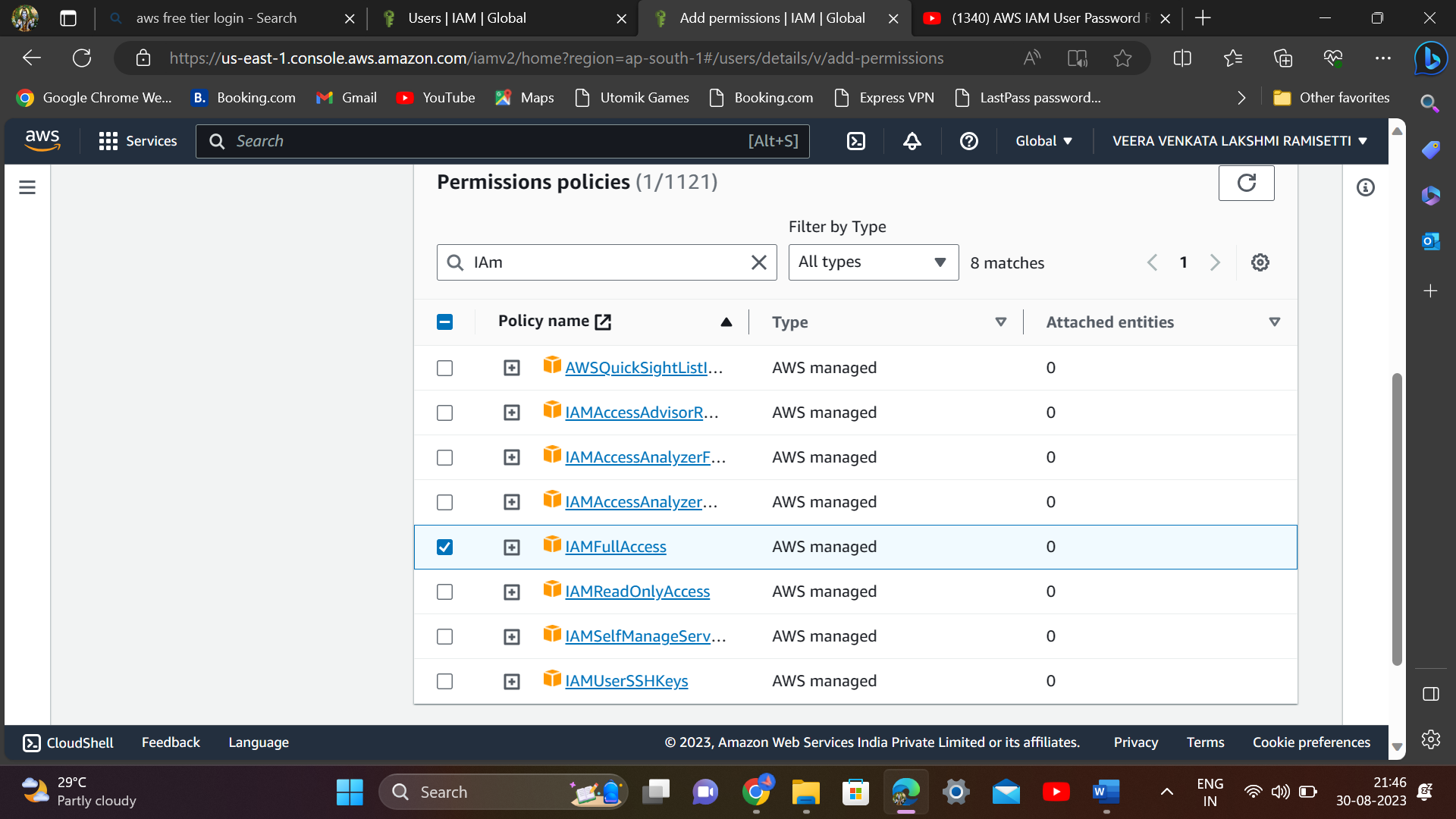


Click on Add permissions

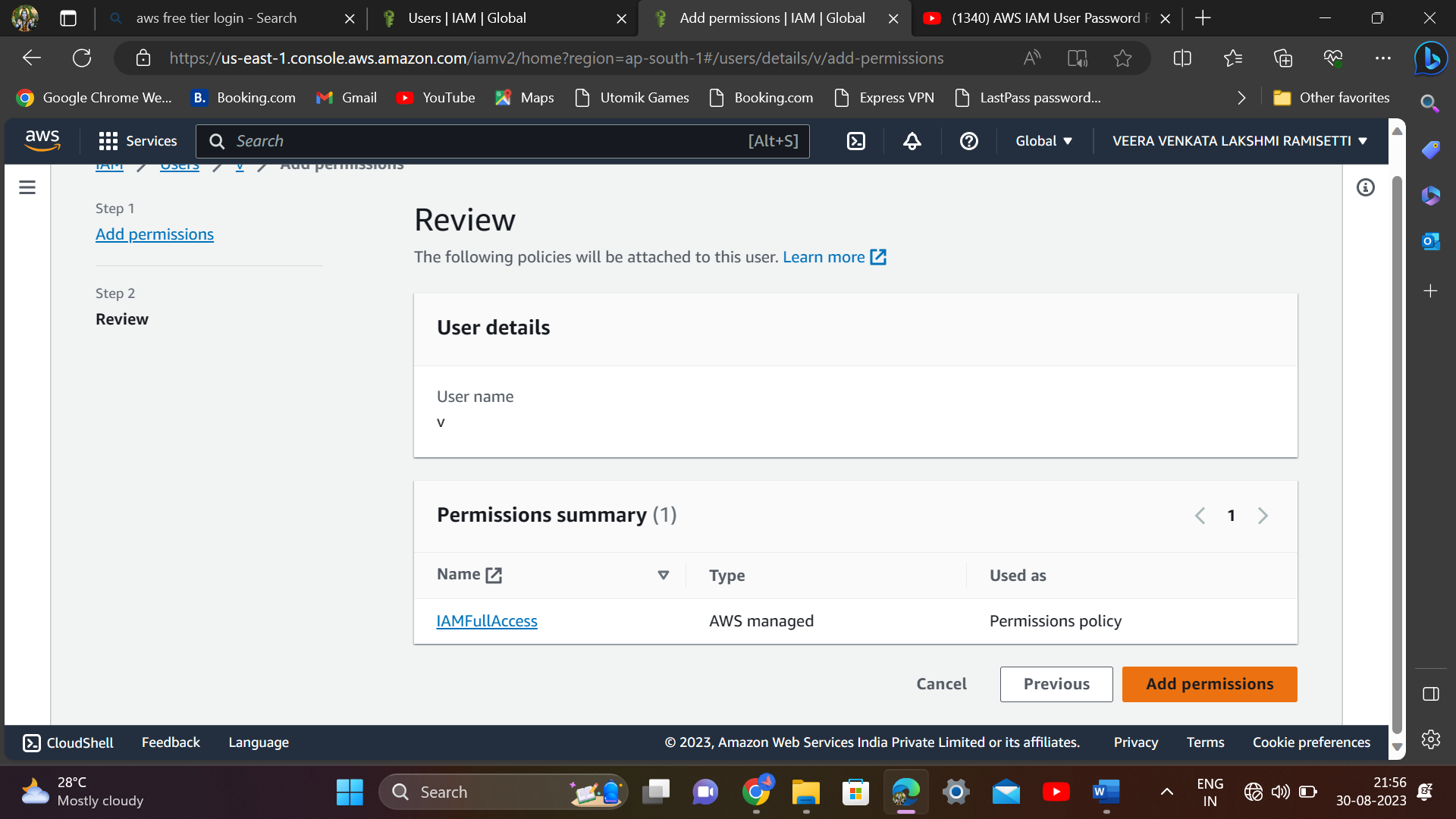


Select attach policies directly option

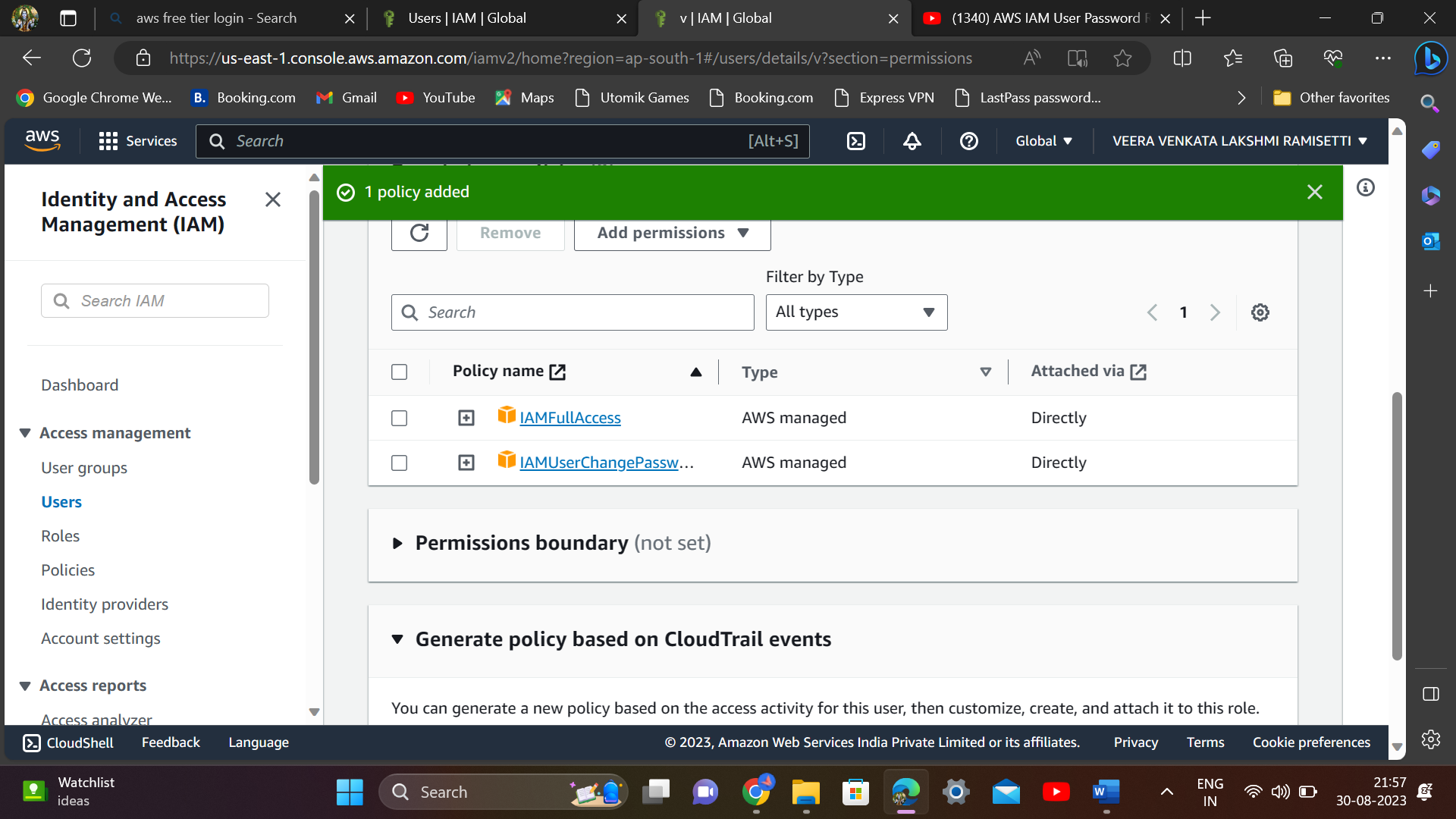
Now search for the service we want to give access



Click on next



Click on add permissions



Policy is successfully added..

That v user has full access of Iam service..means that user has so many access like even they create user,delete his own account..like this

After lab, u have to delete this