

Name → Jahil Jahni

Sci → K

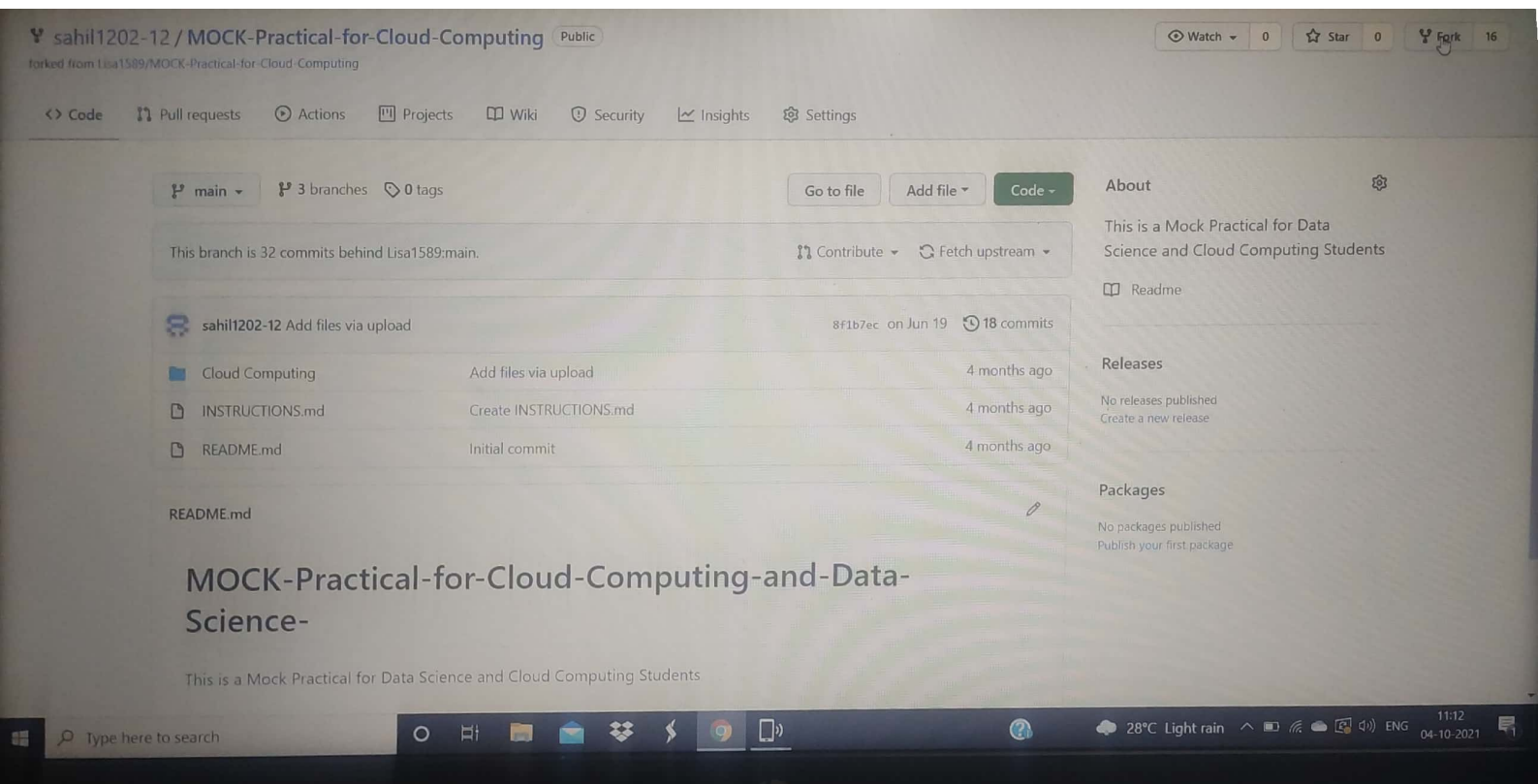
Roll no → 1918637.

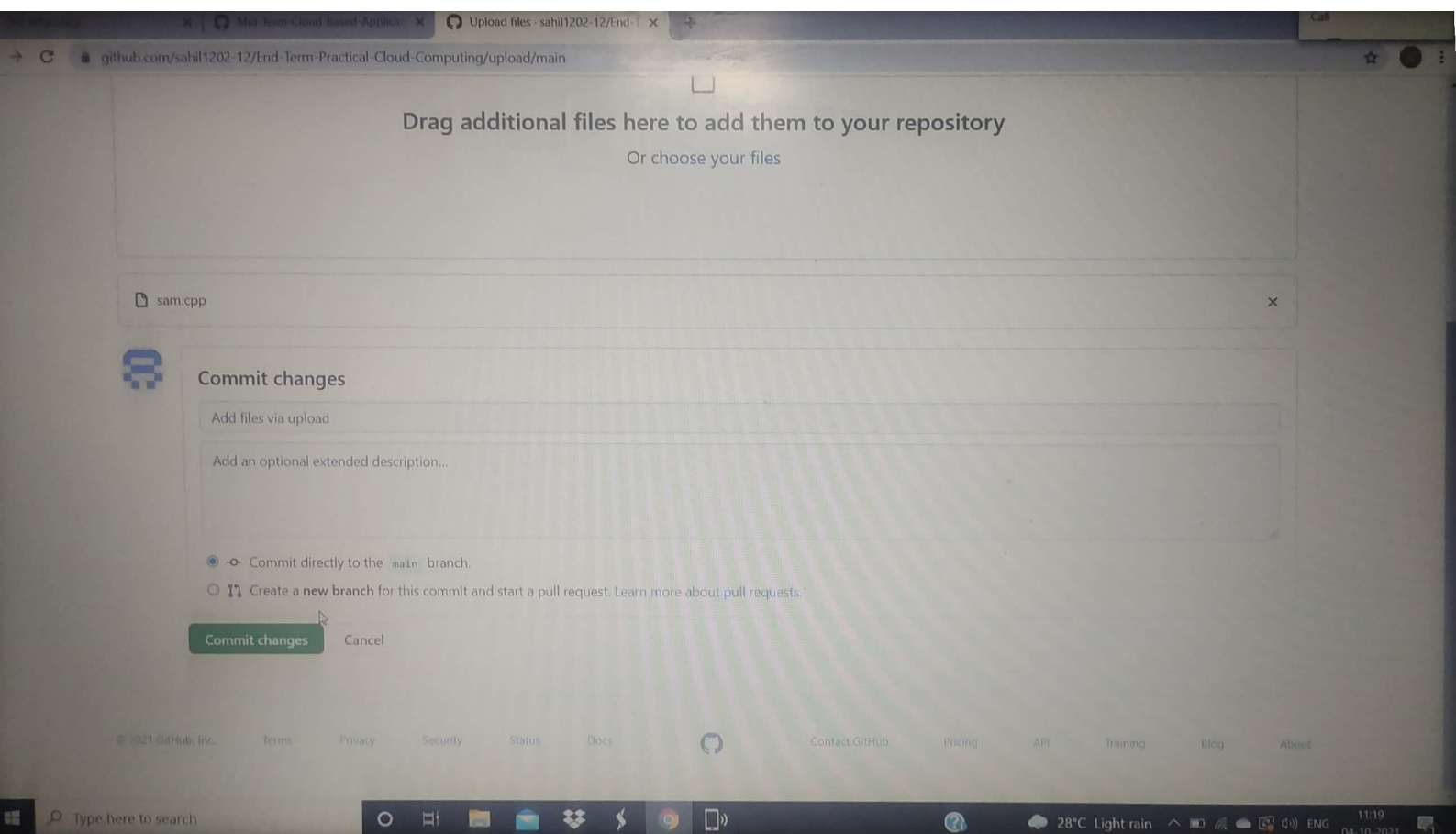
Q3.

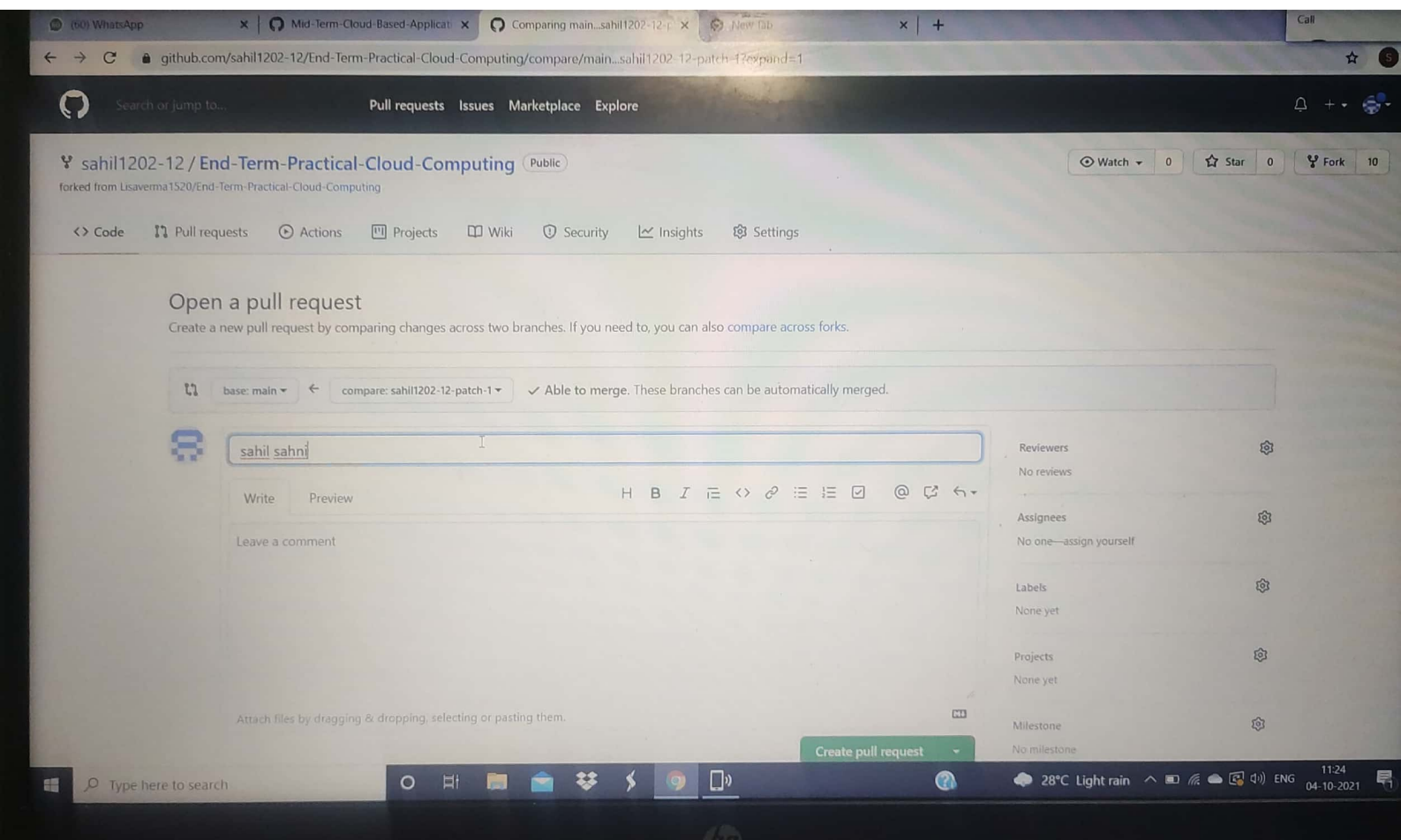
- => 1. Navigate to the original repository where you created your fork.
2. In the 'Branch' menu, choose the branch that contains your commits
3. Above the list of files, click pull request.
4. Use the base branch dropdown menu to select the branch you'd like to merge your changes into, then use the compare branch dropdown menu to choose the topic branch you made changes in.
5. Type a title and description for your pull request
6. To create pull request ready for review click create pull request to create a draft pull request, use the drop down and select create draft pull request then click Draft pull request

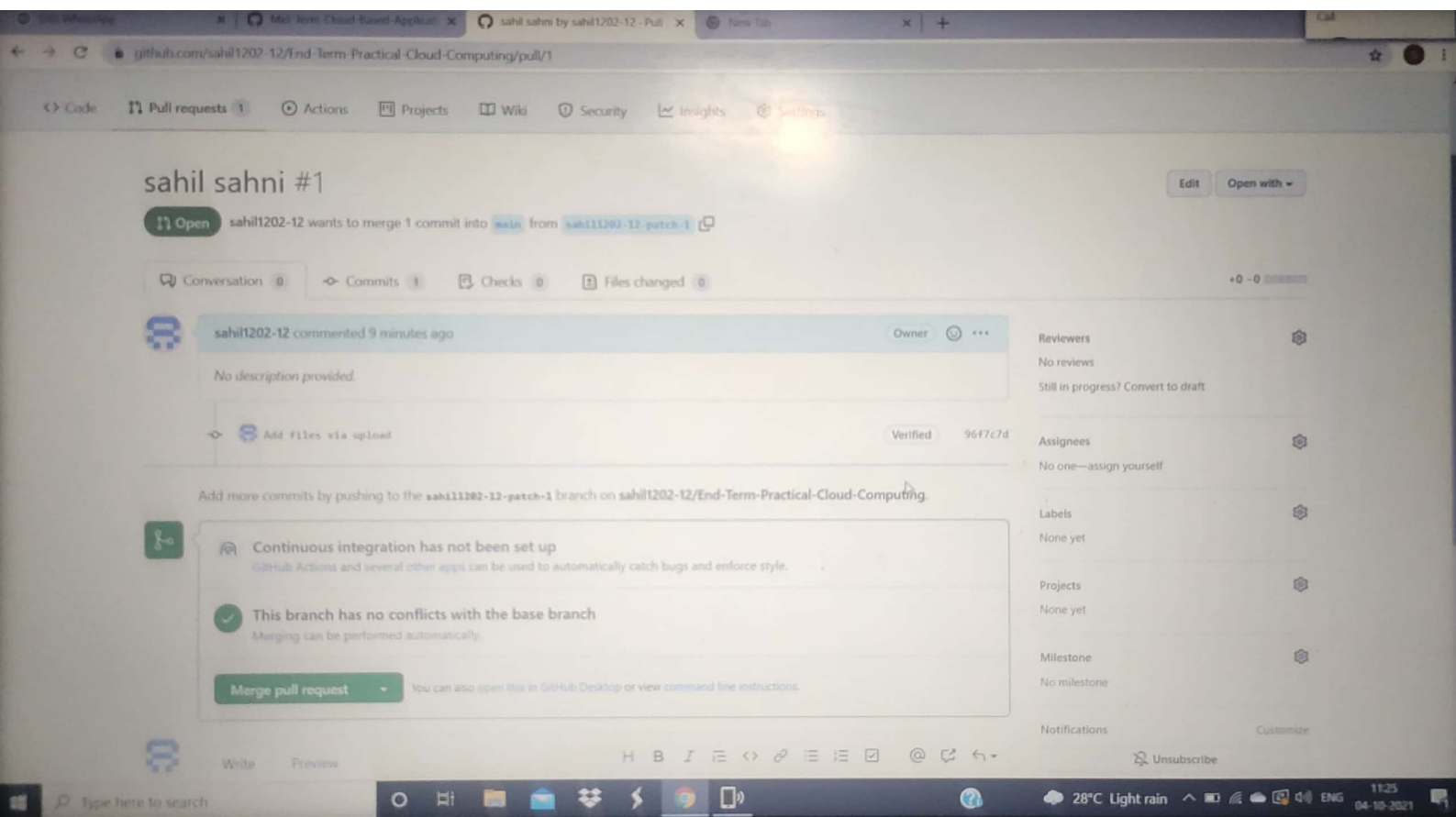
Teacher's Signature : _____

1. After your pull request has been reviewed It can be merged into repository.









Name → Sanil Sanni

Subject Code → PCS-552

Sec → K

Roll no → 1918637

Date → 4/10/21

Q1.

⇒ Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

1. It increases employee and IT productivity
2. It improves security capabilities
3. It combines with Risk-Based Authentication (RBA)
4. It reduces password fatigue
5. It streamlines the user experience.
6. It prevents shadow IT
7. It increases software adoption rates

Teacher's Signature : _____

Steps →

1. Navigate to the AWS IAM Console, and choose AWS accounts from the navigation pane. Choose which account from: Marketing BU organizational unit. Then choose Assign users.

2. Choose User, start typing to search for users, and then choose Search connected directory. This search will return a list of user from connected directory. You can also search for groups.

3. To select permission sets, you first have to create one. Choose Create new permission set.

4. You can use an existing Job Function policy to create a permission set. This type of policy allows you to apply predefined AWS managed policies to permission set that are based on common job functions in IT industry.

5. For this example, choose the Security Audit Job Function policy and then choose Create. As a result, this permission set will be available to pick on the next screen.

6. choose a permission set to indicate what level of access you want to grant your users. For example, assign the Security Audit permission set its created in the previous step to the user choose. Then choose Finish.

7. Your user can sign to the user portal and access the account to which you gave them access. This helps you scale your administrative tasks across multiple AWS accounts.

8. The user can choose an account and a permission set to sign in to that account without needing to provide a password again.

Teacher's Signature : _____

- Dashboard
- AWS accounts**
- Applications
- Connected directory

AWS SSO > AWS Accounts

AWS Accounts

You can configure which users and groups in your connected directory have SSO access to AWS accounts in your AWS organization. You manage permission sets to control the users level of access to these AWS accounts. [Learn more](#)

AWS organization

Permission sets

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. [Learn more](#)

Assign users

to 3 accounts | Deselect

Find AWS account by ID, name, or email

	AWS account	Permission sets
<ul style="list-style-type: none">All accountsRootMarketingBU	<ul style="list-style-type: none">✓ Stage Account 405041790871:5 - awscloudtrail-us-east-1-us-east-1✓ Test Account 49038307117927 - awscloudtrail-us-east-1-us-east-1✓ Production Account 49038307117927 - awscloudtrail-us-east-1-us-east-1	<ul style="list-style-type: none">NoneNoneNone

Assign Users

1

Users and groups

2

Permission sets

Select users or groups

You can search for the users and groups in your connected directory to assign SSO access. Type a user or group name to search in your connected directory. You can also specify an Active Directory domain (optional). You can add more than one user or group to your selection. [Learn more](#)

Groups **Users**

anandcorp.com

Search connected directory

Found 4 matching users

- ✓  jadams
-  jmadison
-  jpolk
-  jtyler

Selection

 anandcorp.com/jadams [Remove](#)

[Cancel](#)

[Next: Permission sets](#)

Assign Users

1

Users and groups

2

Permission sets

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. [Learn more](#)

Create new permission set



Permission set

Description

Provisioned status

Created on

You have not yet created any permission sets.

Create new permission set

How do you want to create your permission set?

☒ Use an existing job function policy

Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. [Learn more](#)

☐ Create a custom permission set

Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. [Learn more](#)

Select job function policy

AdministratorAccess

Provides full access to AWS services and resources.

Billing

Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist

Grants permissions to AWS data analytics services.

Billing

Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist

Grants permissions to AWS data analytics services.

DatabaseAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

NetworkAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

PowerUserAccess

Provides full access to AWS services and resources, but does not allow management of Users and groups.

SecurityAudit

The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SupportUser

This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.

SystemAdministrator

Cancel Create

Assign Users

1

Users and groups

2

Permission sets

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. [Learn more](#)

Create new permission set



✓ Permission set	Description	Provisioned status	Created on
✓ SecurityAudit		Not provisioned	12/5/2017

Cancel

Previous

Finish

Stage Account		Complete	Show details
#650	.com		
Test Account		Complete	Show details
#903	.com		
Production Account		Complete	Show details
#000	.com		

Search



AWS Management Console (3)

650	(Account)	>
903	(Account)	>
68C	(Production Account)	▼
SecurityAudit		

Terms of Use

Powered by AWS



31°C H