NOTE: If you don't have a GitHub account already, you will need to create one and be logged in to GitHub in another browser tab to complete this activity.In your efforts to better support a development organization, you have begun experimenting withGit source control and its interactions with GitHub.

In order to be able to provide secure access to any repositories that are in use, you will create a special SSH key (separate from any that may have been created for other local systems to authenticate through)

to be able to make an exchange with GitHub, and identify a service account called 'cloud\_user'

with your own account.

You will need to use the OpenSSH Client's utilities to create this key.

First, create a subdirectory in your account's home directory called 'githubkeys'.

Using the appropriate tool, you will create a new key (the default encryption type and size will be acceptable according to your organization's security policy) in this new directory called 'github-service-key'.

Once you have this key, find the public key file that matches then copy and paste that into the

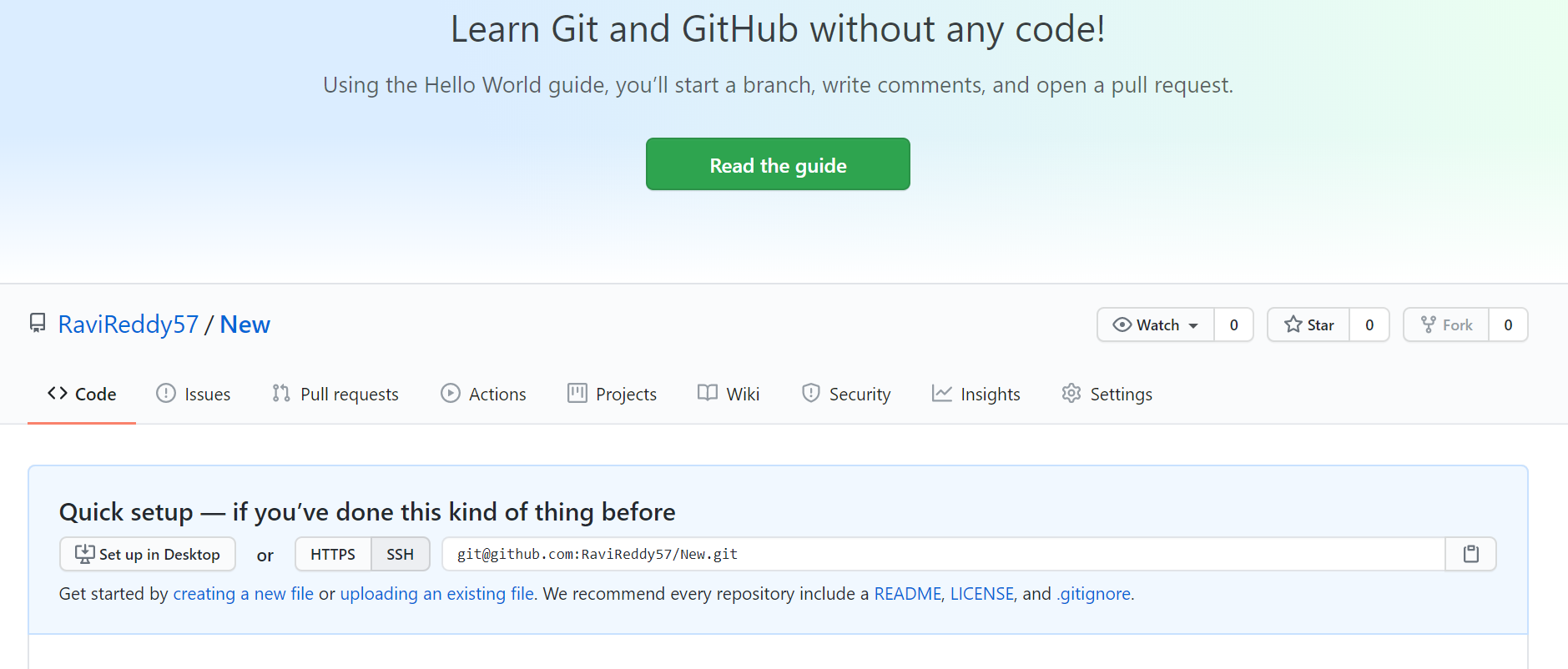
appropriate account profile information in GitHub. After giving the key a reference name,

you should see it appear in the list of your authorized keys, that will confirm

it is available for use when trying to securely connect to your account.

Ans :

Account created in Github.com



SSH part Pending : Need to get some more clarity