ASSIGNMENT 2 BRIEF

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 16: Cloud Computing		
Assignment title	Cloud's implementation and security threats		
Academic Year	2021 – 2022		
Unit Tutor	Ho Hai Van		
Issue date		**Submission date**	
IV name and date			

Submission Format:

Format:

A report (in PDF format)

You must use font *Calibri size 12, set number of the pages and use multiple line spacing at 1.3. Margins must be: left: 1.25 cm; right: 1 cm; top: 1 cm and bottom: 1 cm.* The reference follows Harvard referencing system.

Submission Students are compulsory to submit the assignment in due date and in a way requested by the Tutors. The form of submission will be a soft copy posted on http://cms.greenwich.edu.vn/

Note: The Assignment *must* be your own work, and not copied by or from another student or from books etc. If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. Make sure that you know how to reference properly, and that understand the guidelines on plagiarism. *If you do not, you definitely get failed*

Unit Learning Outcomes:

LO3 Develop Cloud Computing solutions using service provider's frameworks and open source tools.

LO4 Analyze the technical challenges for cloud applications and assess their risks

Assignment Brief and Guidance:

Task 1

Base on the scenario and architecture design in the first assignment provide the implementation. Because of the time constraint of the assignment, the implementation just provides some demo functions of the scenario. The implementation includes two parts:

- A step-by-step instruction
  - which shows which functions are implemented
  - How to config, deploy and test the services (Web application, Database Server, Source code management, server logs...) using service provider's frameworks and open-source tools.
  - Images for the built functions
- A brief discussion about difficulties which one can face during the development process(optional)
- The source code for the built application

Task 2

The table of contents in your security manual (which should be 500–700 words) should be as follows:

1. Analysis of the most **common problems** and **security issues** of a cloud computing platform.
2. Discussion on how to overcome these issues.
3. Summary.

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO3 Develop Cloud Computing solutions using service provider's frameworks and open-source tools		**D2** Critically discuss how one can overcome these issues and constraints.
P5 Configure a Cloud Computing platform with a cloud service provider's framework. **P6** Implement a cloud platform using open-source tools.	**M3** Discuss the issues and constraints one can face during the development process.	
LO4 Analyse the technical challenges for cloud applications and assess their risks		
P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems. **P8** Assess the most common security issues in cloud environments.	**M4** Discuss how to overcome these security issues when building a secure cloud platform.	**D3** Critically discuss how an organisation should protect their data when they migrate to a cloud solution.

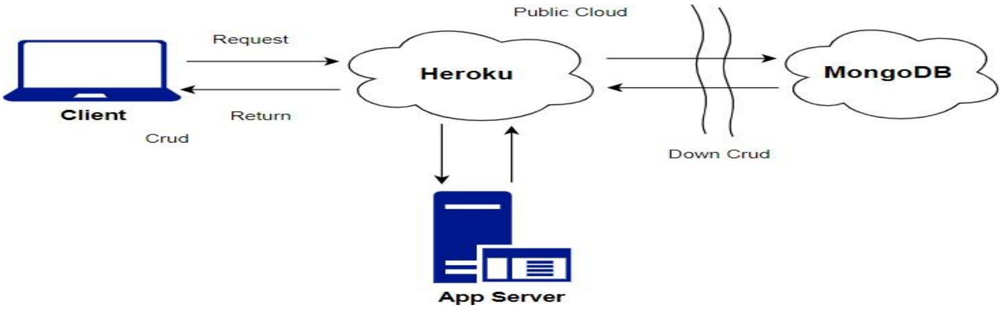
Table of Contents

P5. Configure a Cloud Computing platform with a cloud service provider’s framework.

1. Introducing configurable cloud.

Provide the implementation based on the first assignment's scenario and architectural design. On the cloud environment, we integrate Node.js with Heroku and mongoDB. Subsequently, we initiate the procedure, develop the cloud server, install the cloud software, generate the database, and locate the required data.

1.1. Design Cloud Server.

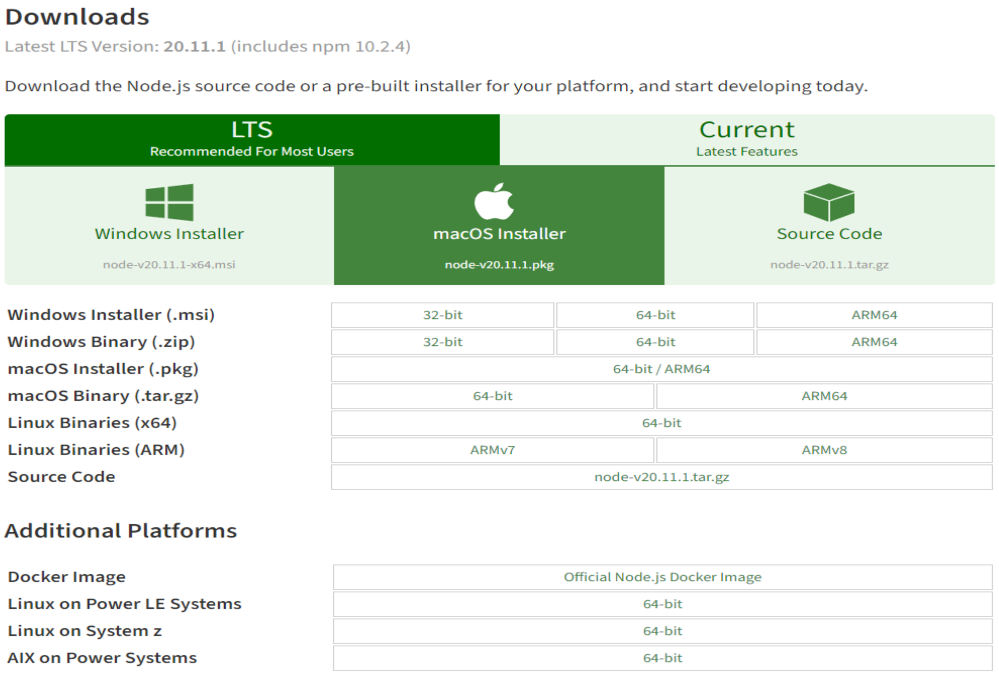


1.2. Installation Node.js

Step 1: Link download Node.js

https://nodejs.org/en/download/

You may select the program based on your preferred operating system.



Downloads

Latest LTS Version: **20.11.1** (includes npm 10.2.4)

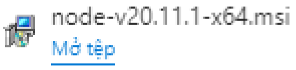
Download the Node.js source code or a pre-built installer for your platform, and start developing today.

Windows Installer (.msi)	32-bit	64-bit	ARM64
Windows Binary (.zip)	32-bit	64-bit	ARM64
macOS Installer (.pkg)	64-bit / ARM64		
macOS Binary (.tar.gz)	64-bit	ARM64	
Linux Binaries (x64)	64-bit		
Linux Binaries (ARM)	ARMv7	ARMv8	
Source Code	node-v20.11.1.tar.gz		

Additional Platforms

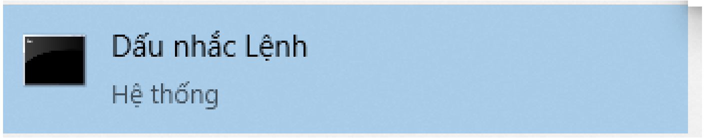
Docker Image	Official Node.js Docker Image
Linux on Power LE Systems	64-bit
Linux on System z	64-bit
AIX on Power Systems	64-bit

Step 2: Launch Nodejs.exe. As with other applications, it should be installed by default on the C drive.



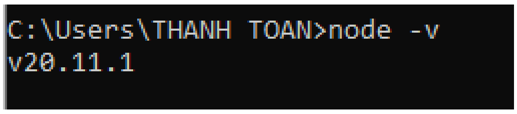
node-v20.11.1-x64.msi
Mở tệp

Step 3: Search cmd on windows, and open cmd by on click run as mindistrator.



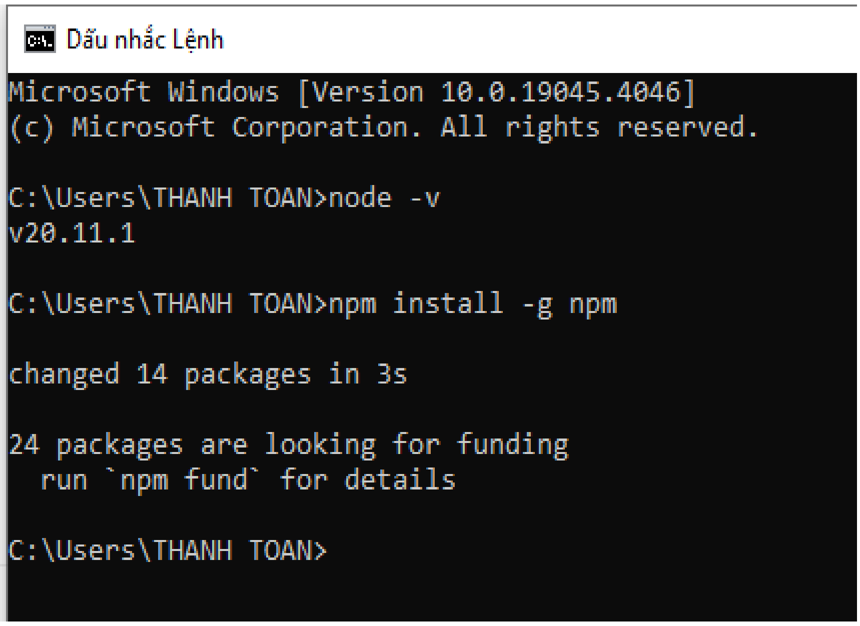
Dấu nhắc Lệnh
Hệ thống

Step 4: Check version of Node.js



```
C:\Users\THANH TOAN>node -v
v20.11.1
```

Step 5: Install libraries for Node.js

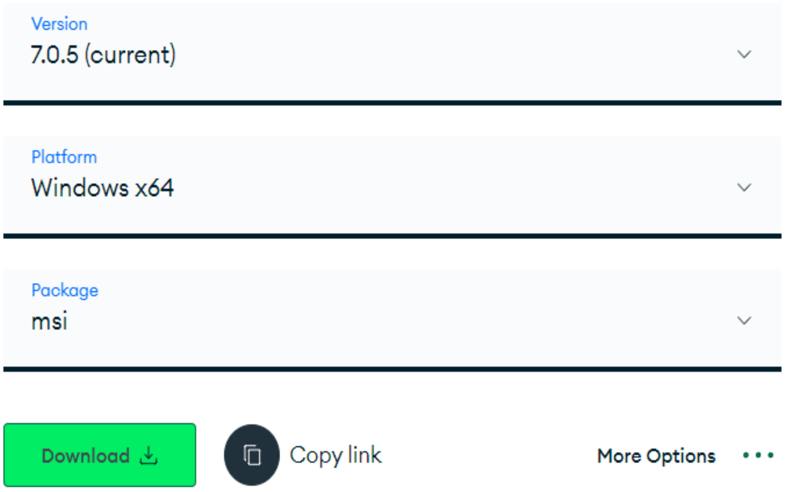


Dấu nhắc Lệnh

```
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\THANH TOAN>node -v
v20.11.1

C:\Users\THANH TOAN>npm install -g npm

changed 14 packages in 3s

24 packages are looking for funding
  run `npm fund` for details

C:\Users\THANH TOAN>
```

1.3. Installation MongoDB

Step 1: Link Download MongoDB https://www.mongodb.com/try/download/community

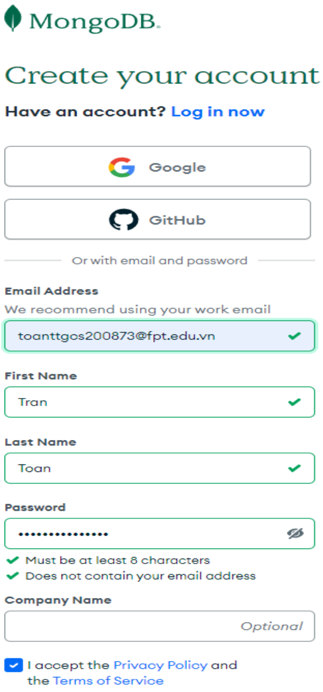


Version: 7.0.5 (current)

Platform: Windows x64

Package: msi

Step 2: Sign up MongoDB



Create your account

Have an account? Log in now

Email Address
We recommend using your work email
toanttgcs200873@fpt.edu.vn ✓

First Name
Tran ✓

Last Name
Toan ✓

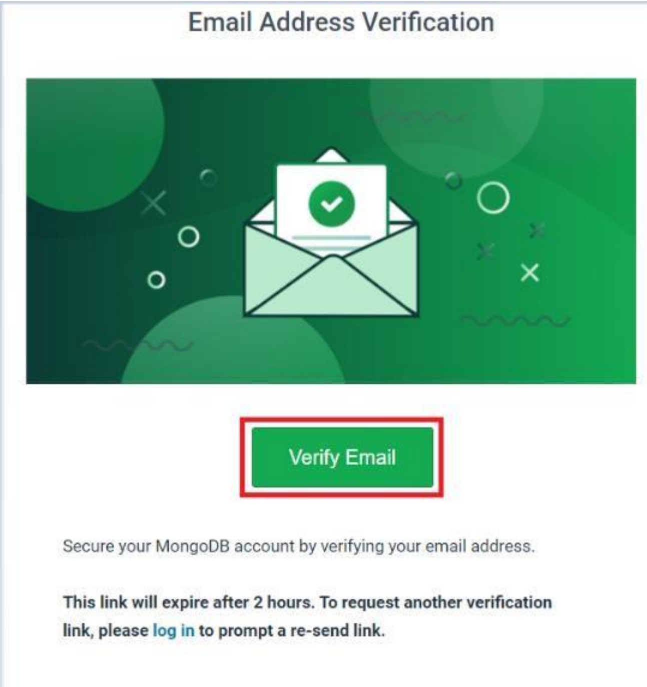
Password
•••••••••••••••

✓ Must be at least 8 characters
✓ Does not contain your email address

Company Name
Optional

☑ I accept the Privacy Policy and the Terms of Service

Step 3: You confirm gmail when you have successfully registered.



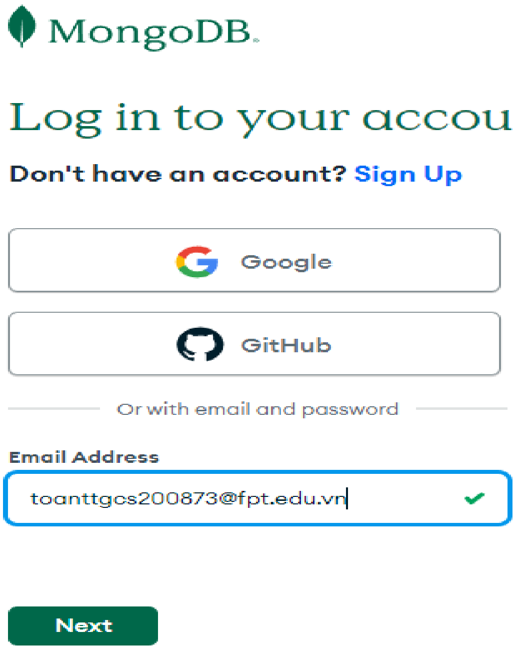
Email Address Verification

Secure your MongoDB account by verifying your email address.

This link will expire after 2 hours. To request another verification link, please log in to prompt a re-send link.

Step 4: Login had created MongoDB by Google

https://account.mongodb.com/account/login



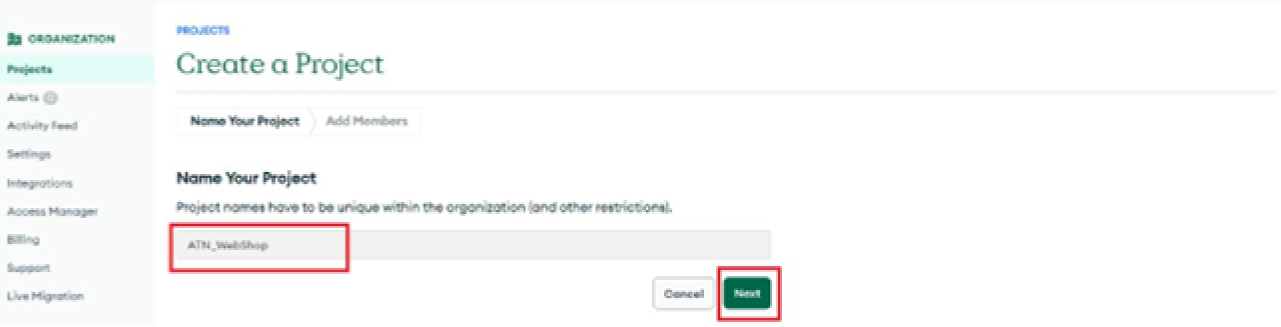
Log in to your account

Don't have an account? Sign Up

Email Address

toanttgcs200873@fpt.edu.vn

Step 5: Create a new Project by Web MongoDB



ORGANIZATION
Projects
Alerts
Activity Feed
Settings
Integrations
Access Manager
Billing
Support
Live Migration

PROJECTS

Create a Project

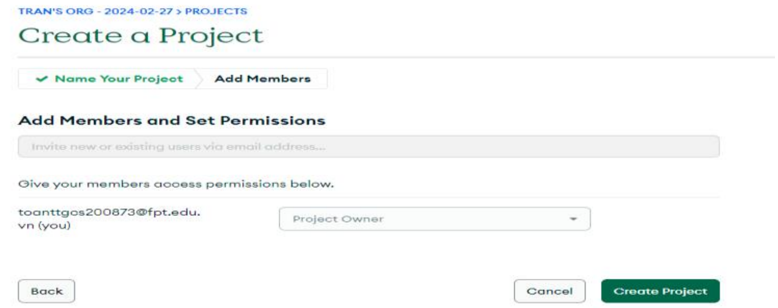
Name Your Project > Add Members

Name Your Project

Project names have to be unique within the organization (and other restrictions).

ATN_WebShop

Cancel Next



TRAN'S ORG - 2024-02-27 > PROJECTS

Create a Project

✓ Name Your Project > Add Members

Add Members and Set Permissions

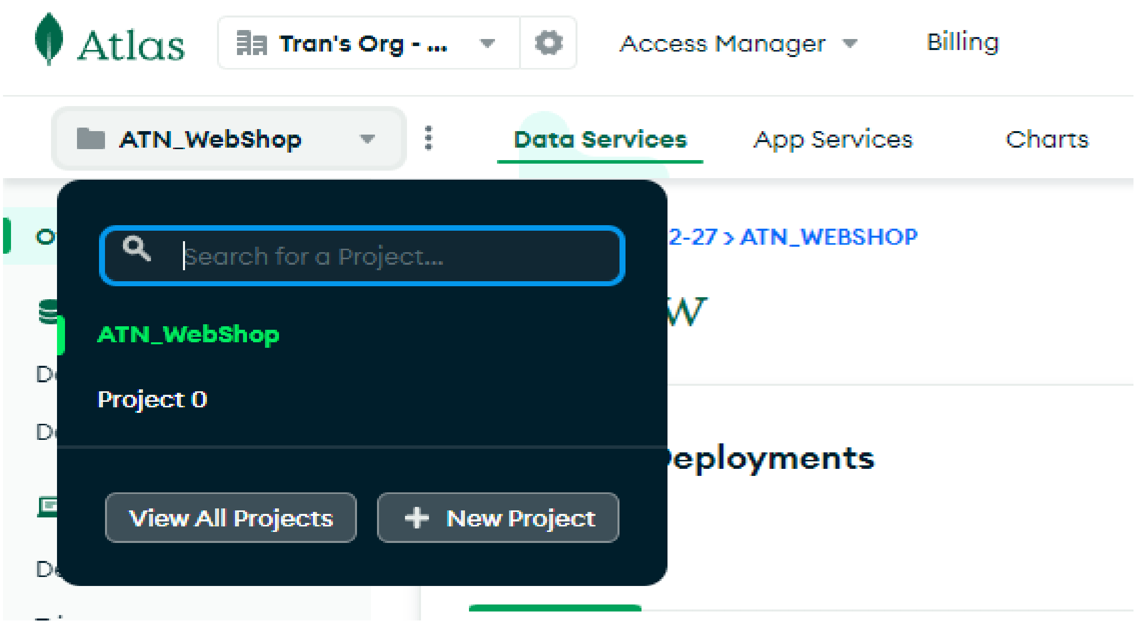
Invite new or existing users via email address...

Give your members access permissions below.

toanttgos200873@fpt.edu.vn (you) — Project Owner

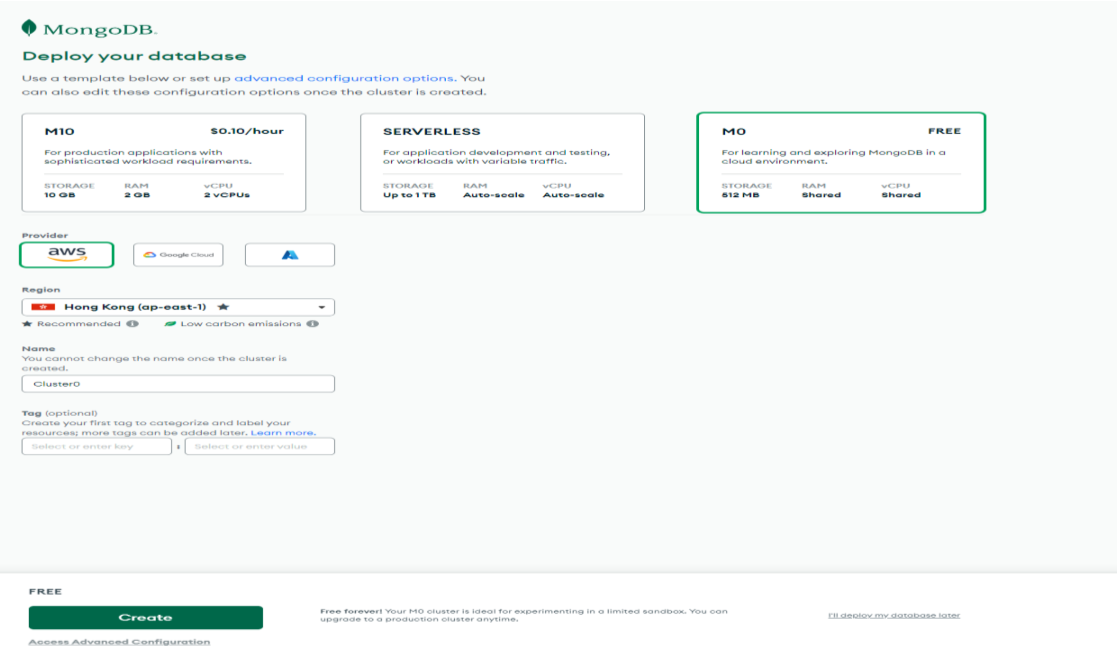
Back Cancel Create Project

Step 6: Choose the created project ATN_WebShop



Atlas
Tran's Org - ...
Access Manager
Billing
ATN_WebShop
Data Services
App Services
Charts
Search for a Project...
ATN_WebShop
Project 0
View All Projects
+ New Project
2-27 > ATN_WEBSHOP
eployments

Step 7: Build a Database



MongoDB.

Deploy your database

Use a template below or set up advanced configuration options. You can also edit these configuration options once the cluster is created.

M10 $0.10/hour
For production applications with sophisticated workload requirements.

STORAGE	RAM	vCPU
10 GB	2 GB	2 vCPUs

SERVERLESS
For application development and testing, or workloads with variable traffic.

STORAGE	RAM	vCPU
Up to 1 TB	Auto-scale	Auto-scale

M0 FREE
For learning and exploring MongoDB in a cloud environment.

STORAGE	RAM	vCPU
512 MB	Shared	Shared

Provider
aws | Google Cloud

Region
Hong Kong (ap-east-1) ★
★ Recommended · Low carbon emissions

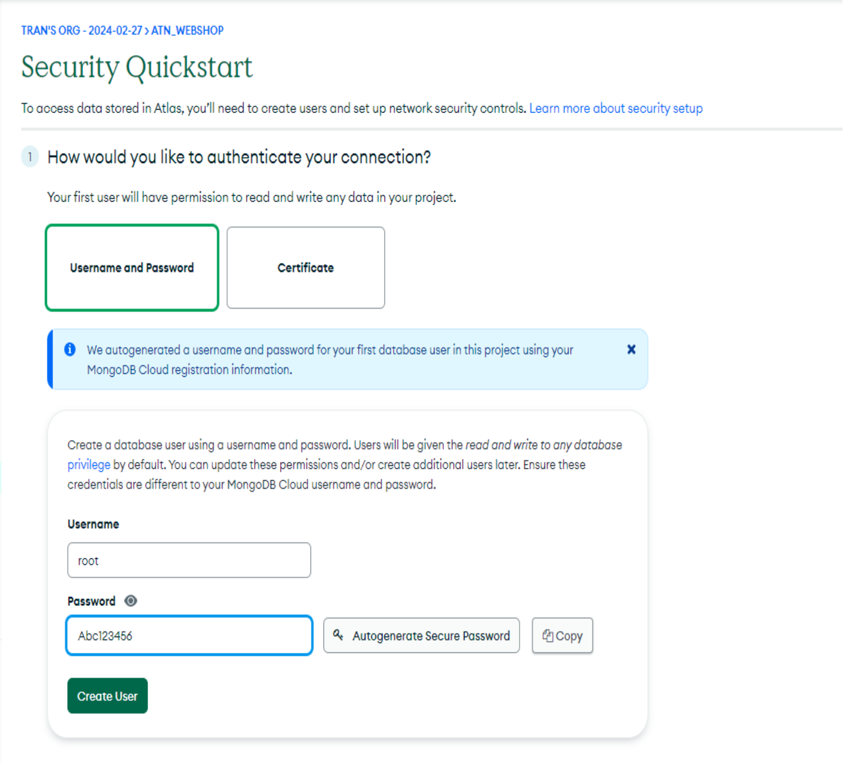
Name
You cannot change the name once the cluster is created.
Cluster0

Tag (optional)
Create your first tag to categorize and label your resources; more tags can be added later. Learn more.
Select or enter key : Select or enter value

FREE
Create
Access Advanced Configuration

Free forever! Your M0 cluster is ideal for experimenting in a limited sandbox. You can upgrade to a production cluster anytime.

I'll deploy my database later



TRAN'S ORG - 2024-02-27 > ATN_WEBSHOP

Security Quickstart

To access data stored in Atlas, you'll need to create users and set up network security controls. Learn more about security setup

1 How would you like to authenticate your connection?

Your first user will have permission to read and write any data in your project.

Username and Password | Certificate

We autogenerated a username and password for your first database user in this project using your MongoDB Cloud registration information.

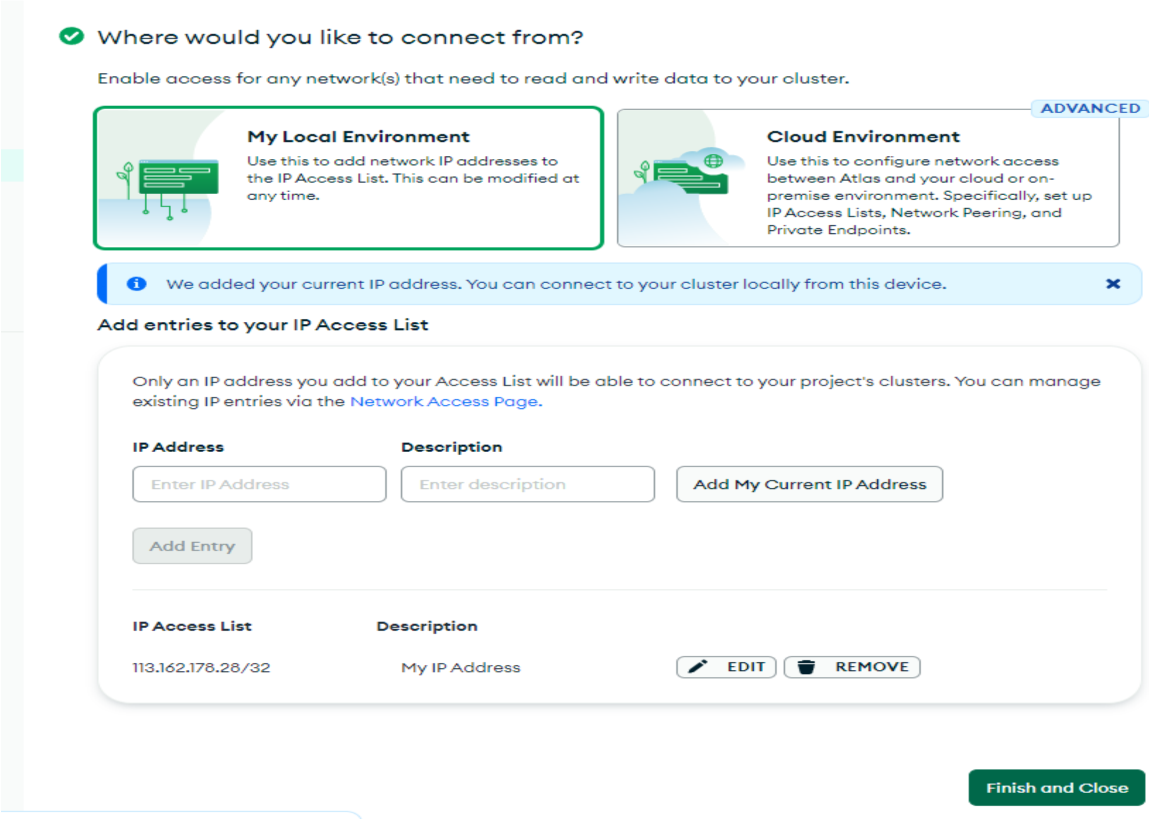
Create a database user using a username and password. Users will be given the *read and write to any database* privilege by default. You can update these permissions and/or create additional users later. Ensure these credentials are different to your MongoDB Cloud username and password.

Username
root

Password
Abc123456

Autogenerate Secure Password | Copy

Create User



Where would you like to connect from?

Enable access for any network(s) that need to read and write data to your cluster.

My Local Environment
Use this to add network IP addresses to the IP Access List. This can be modified at any time.

ADVANCED
Cloud Environment
Use this to configure network access between Atlas and your cloud or on-premise environment. Specifically, set up IP Access Lists, Network Peering, and Private Endpoints.

We added your current IP address. You can connect to your cluster locally from this device.

Add entries to your IP Access List

Only an IP address you add to your Access List will be able to connect to your project's clusters. You can manage existing IP entries via the Network Access Page.

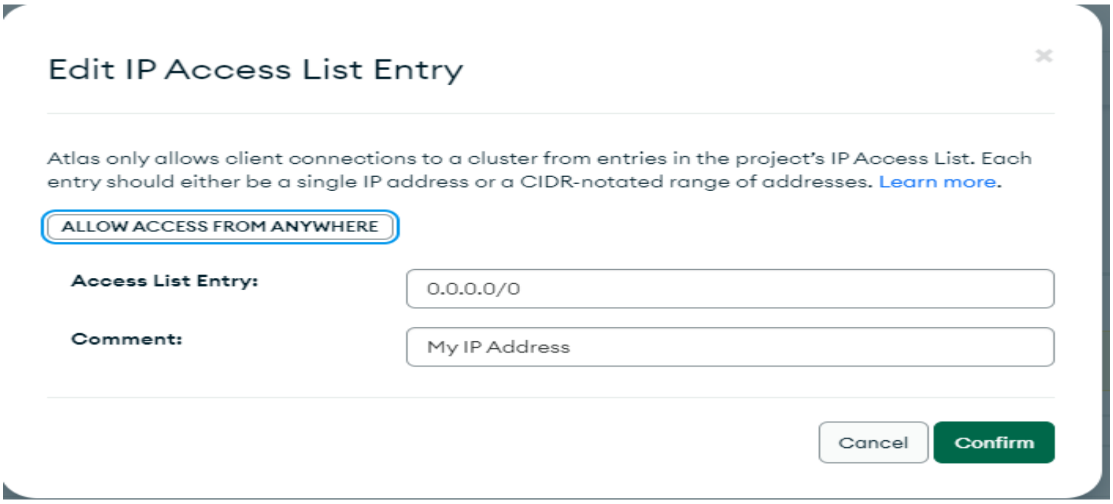
IP Address	Description	
Enter IP Address	Enter description	Add My Current IP Address

Add Entry

IP Access List	Description	
113.162.178.28/32	My IP Address	EDIT REMOVE

Finish and Close

Step 8 : Add IP Access List Entry of mongoDB. When create add ip address.



Edit IP Access List Entry

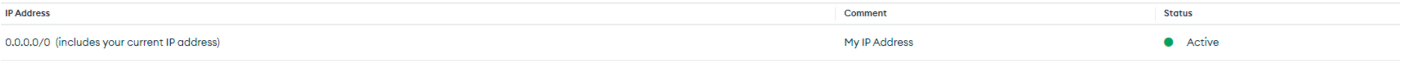
Atlas only allows client connections to a cluster from entries in the project's IP Access List. Each entry should either be a single IP address or a CIDR-notated range of addresses. Learn more.

ALLOW ACCESS FROM ANYWHERE

Access List Entry: 0.0.0.0/0

Comment: My IP Address

Cancel Confirm



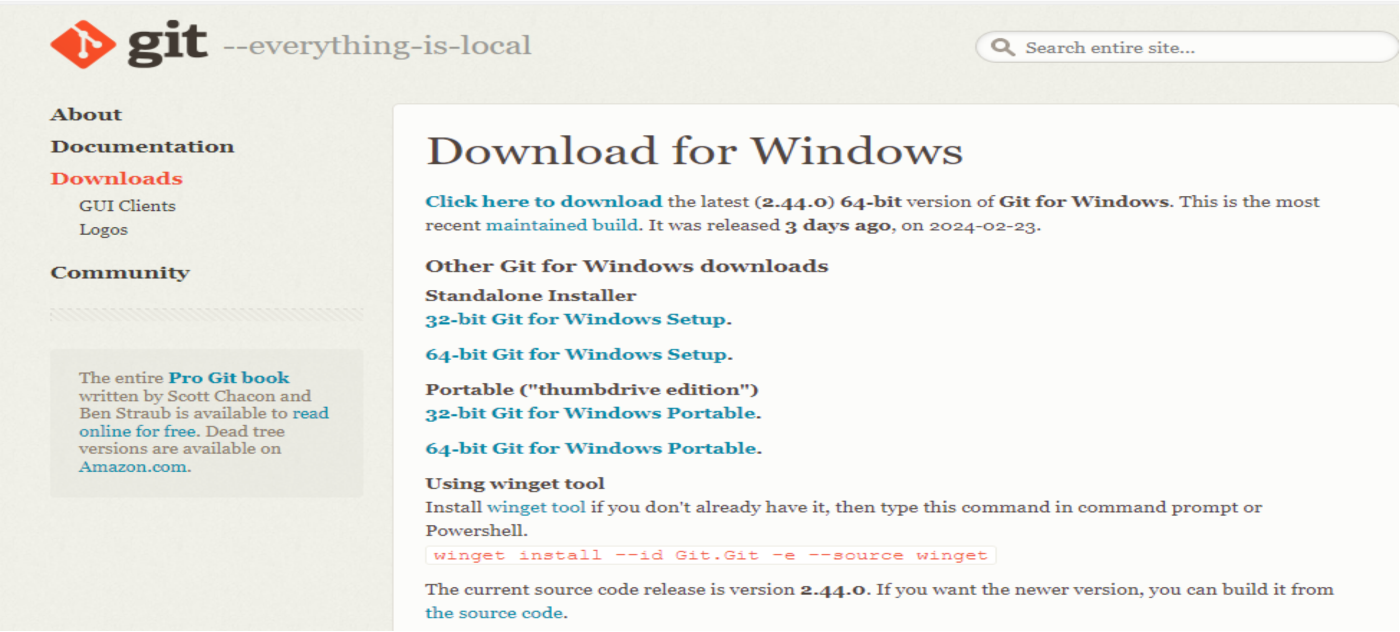
IP Address	Comment	Status
0.0.0.0/0 (includes your current IP address)	My IP Address	● Active

Connection Successful

1.4. Installation Git and Github

Step 1: Link download git

https://git-scm.com/download/win



git --everything-is-local

Search entire site...

About
Documentation
Downloads
GUI Clients
Logos
Community

The entire Pro Git book written by Scott Chacon and Ben Straub is available to read online for free. Dead tree versions are available on Amazon.com.

Download for Windows

Click here to download the latest (2.44.0) 64-bit version of Git for Windows. This is the most recent maintained build. It was released 3 days ago, on 2024-02-23.

Other Git for Windows downloads

Standalone Installer

32-bit Git for Windows Setup.

64-bit Git for Windows Setup.

Portable ("thumbdrive edition")

32-bit Git for Windows Portable.

64-bit Git for Windows Portable.

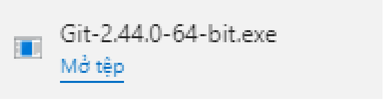
Using winget tool

Install winget tool if you don't already have it, then type this command in command prompt or Powershell.

```
winget install --id Git.Git -e --source winget
```

The current source code release is version 2.44.0. If you want the newer version, you can build it from the source code.

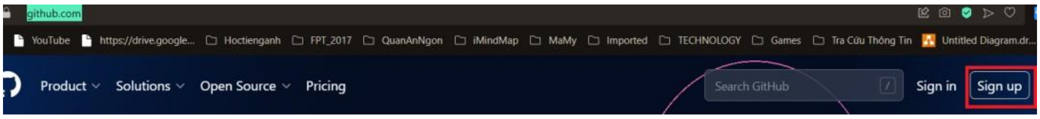
Step 2: Setup Git



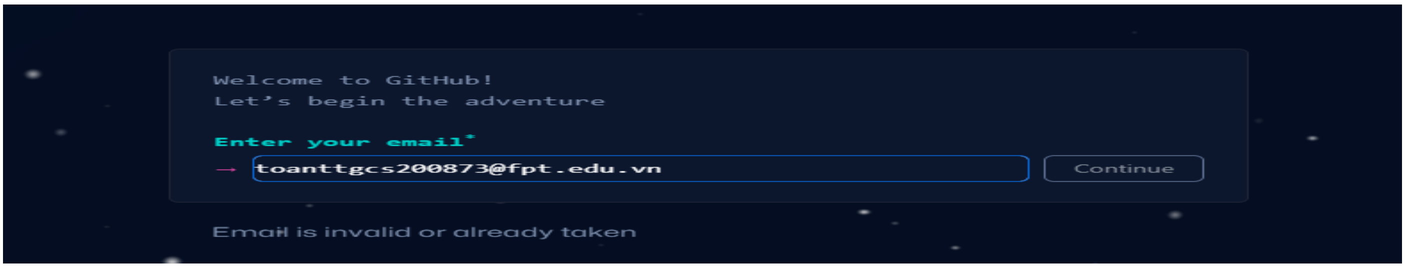
Git-2.44.0-64-bit.exe
Mở tệp

Step 3: Sign up GitHub

Link: https://github.com



Step 4: Create a password for your new GitHub account, and Enter a username, too. Next, choose whether you want to receive updates and announcements via email, and then select Continue.



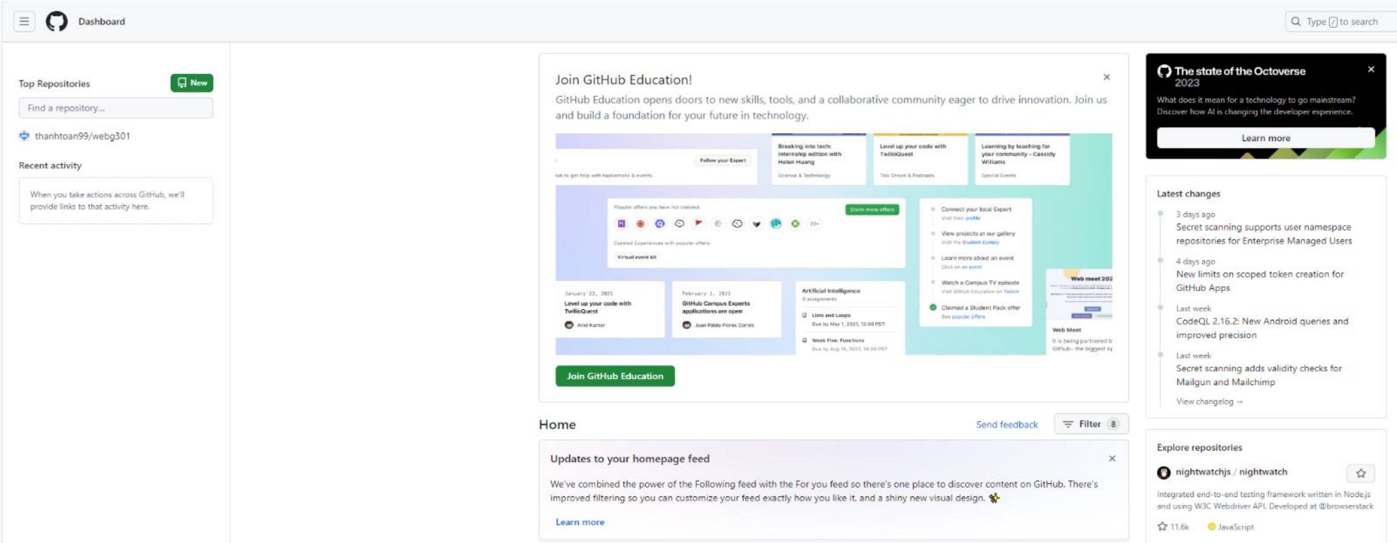
Welcome to GitHub!
Let's begin the adventure

Enter your email*
→ toanttgcs200873@fpt.edu.vn

Email is invalid or already taken

Step 5: Verify your account by solving a puzzle. Select the Start Puzzle button to do so, and then follow the prompts. After you verify your account, select the Create account button. Next, GitHub sends a launch code to your email address. Type that launch code in the Enter code dialog, and then press Enter.

Step 6: Create repository new, choose Public, and Create repository. Other than that, you don't need to choose anything.



Top Repositories

thanhtoan99/webg301

Recent activity

When you take actions across GitHub, we'll provide links to that activity here.

Join GitHub Education!

GitHub Education opens doors to new skills, tools, and a collaborative community eager to drive innovation. Join us and build a foundation for your future in technology.

Home

Updates to your homepage feed

We've combined the power of the Following feed with the For you feed so there's one place to discover content on GitHub. There's improved filtering so you can customize your feed exactly how you like it, and a shiny new visual design. ✨

The state of the Octoverse 2023

What does it mean for a technology to go mainstream? Discover how AI is changing the developer experience.

Latest changes

3 days ago
Secret scanning supports user namespace repositories for Enterprise Managed Users

4 days ago
New limits on scoped token creation for GitHub Apps

Last week
CodeQL 2.16.2: New Android queries and improved precision

Last week
Secret scanning adds validity checks for Mailgun and Mailchimp

Explore repositories

nightwatchjs / nightwatch

Integrated end-to-end testing framework written in Node.js and using W3C Webdriver API. Developed at @browserstack

11.6k JavaScript

Dashboard
Type / to search
New
Find a repository...
Follow your Expert
Breaking into tech: internship edition with Helen Huang
Level up your code with TwilioQuest
Learning by teaching for your community - Cassidy Williams
Claim more offers
Virtual event kit
Connect your local Expert
View projects at our gallery
Learn more about an event
Watch a Campus TV episode
Claimed a Student Pack offer
January 22, 2021
Level up your code with TwilioQuest
February 1, 2021
GitHub Campus Experts applications are open
Artificial Intelligence
Lists and Loops
Week Five: Functions
Web Meet
Join GitHub Education
Send feedback
Filter 8
Learn more
Learn more
View changelog →

P6. Implement a cloud platform using open-source tools.

1. Installs Program library.

Note

Step 1: Install framework for nodejs

npm install --save express

Step 2: Install the Cloud-Native Document Database as a MongoDB Service

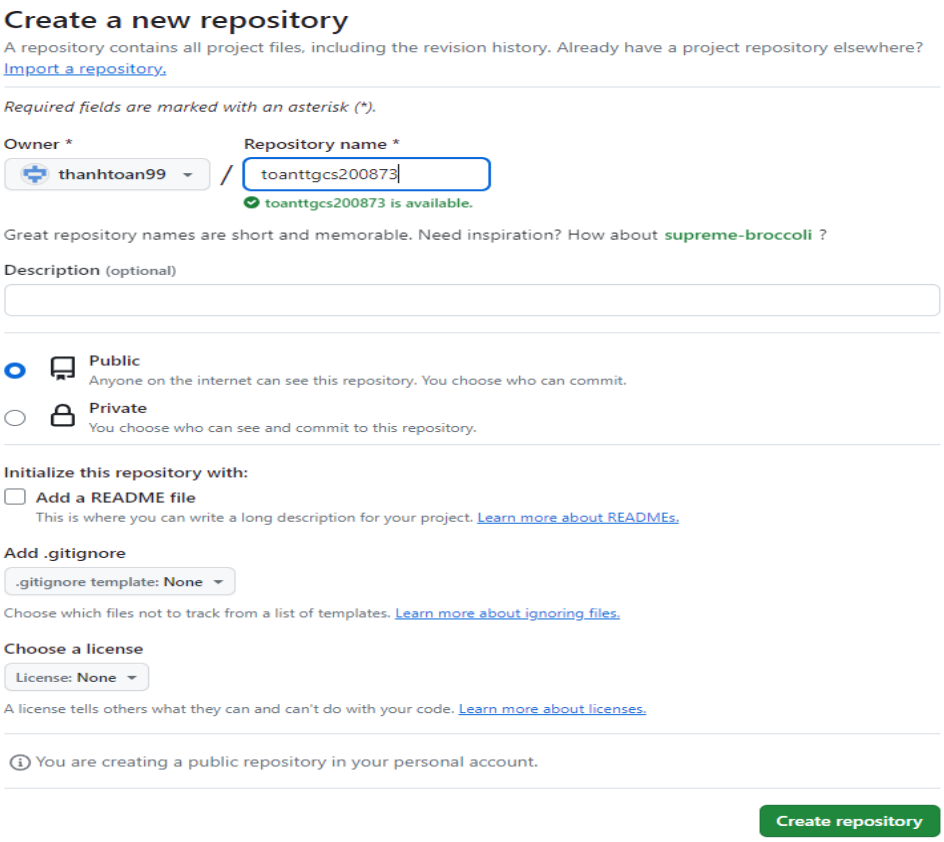
npm install mongodb –save

Step 3: Push entered data to HTML using body-parser

npm install body-parser –save

Step 4: EJS is a JavaScript library designed to support the task of templating

npm install ejs –save



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? Import a repository.

Required fields are marked with an asterisk (*).

Owner * thanhtoan99 / Repository name * toanttgcs200873

toanttgcs200873 is available.

Great repository names are short and memorable. Need inspiration? How about supreme-broccoli ?

Description (optional)

● Public
Anyone on the internet can see this repository. You choose who can commit.

○ Private
You choose who can see and commit to this repository.

Initialize this repository with:

□ Add a README file
This is where you can write a long description for your project. Learn more about READMEs.

Add .gitignore

.gitignore template: None

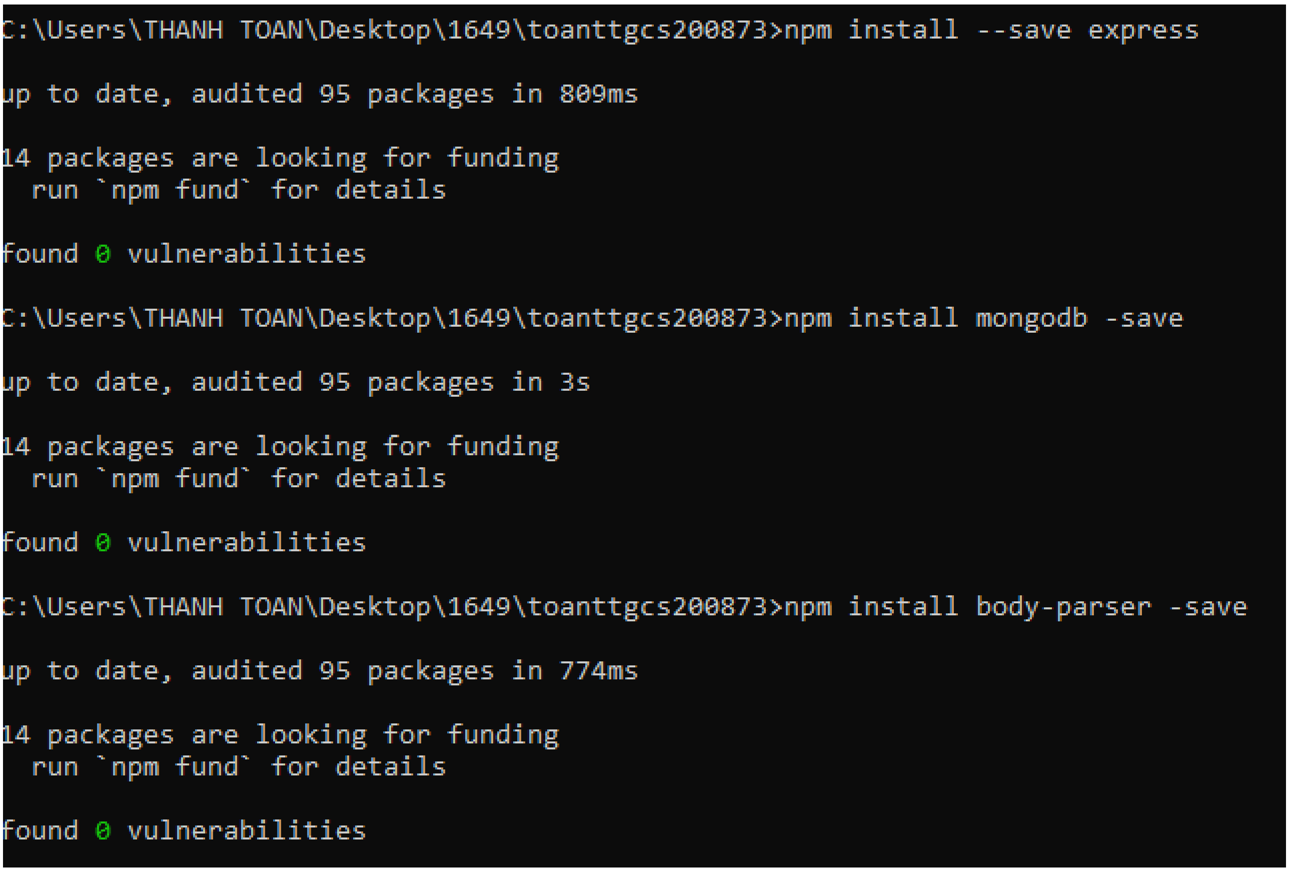
Choose which files not to track from a list of templates. Learn more about ignoring files.

Choose a license

License: None

A license tells others what they can and can't do with your code. Learn more about licenses.

You are creating a public repository in your personal account.



```
C:\Users\THANH TOAN\Desktop\1649\toanttgcs200873>npm install --save express

up to date, audited 95 packages in 809ms

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\THANH TOAN\Desktop\1649\toanttgcs200873>npm install mongodb -save

up to date, audited 95 packages in 3s

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\THANH TOAN\Desktop\1649\toanttgcs200873>npm install body-parser -save

up to date, audited 95 packages in 774ms

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

2. Nodejs Push GitHub.

Note

Push an existing repository from the command line

Step 1: "origin" is the local name of the remote repository.

git remote add origin

Step 2: The git branch command does more than just create and delete branches

git branch -M main

Step 3: Origin refers to the repository on GitHub (aka the "remote repository") where you originally cloned your code from.

git push -u origin main

Step 4: Waiting for js code to be pushed to Github.

Step 5: Update Code Github

The git add command adds new or changed files in your working directory to the Git staging area.

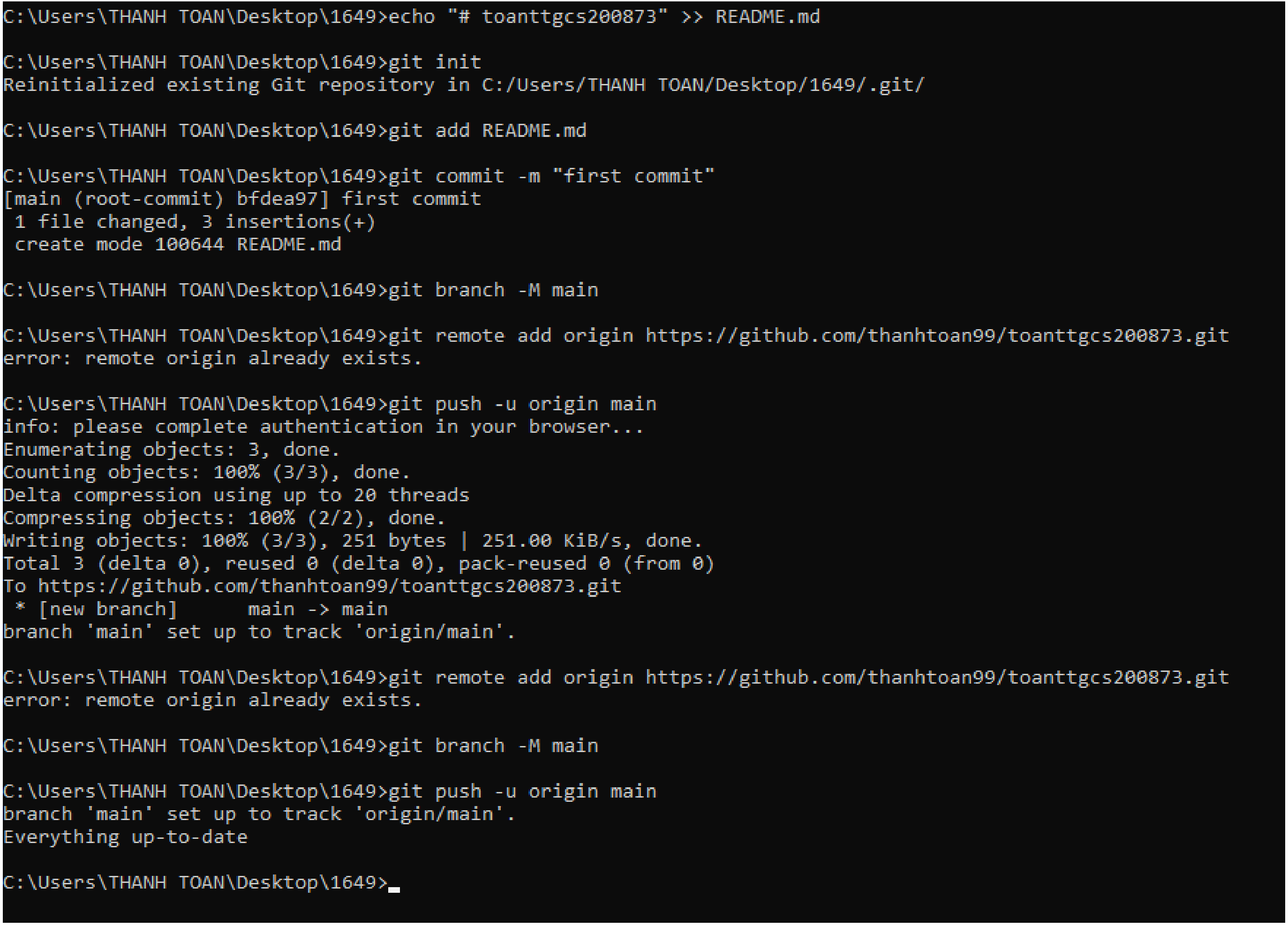
git add .

In version control systems, a commit is an operation which sends the latest changes of the source code to the repository

git commit -m “update github”

Use the git push command to push the code from your local repository's main branchto your

git push

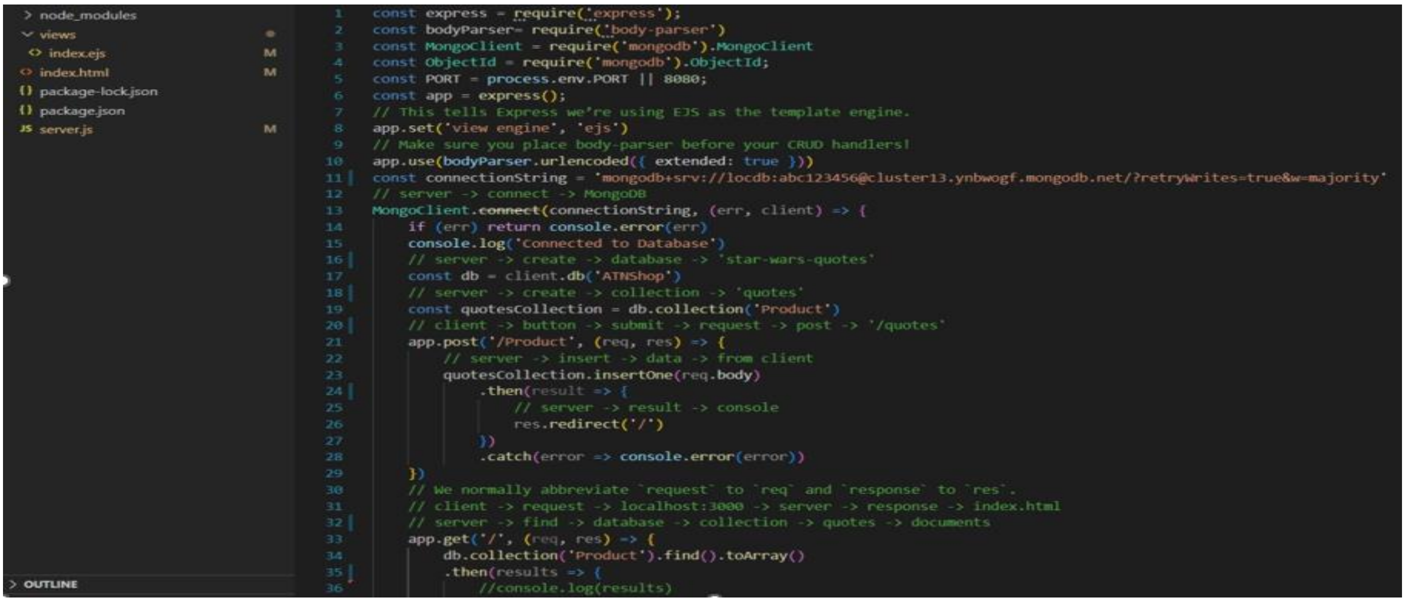


```
C:\Users\THANH TOAN\Desktop\1649>echo "# toanttgcs200873" >> README.md

C:\Users\THANH TOAN\Desktop\1649>git init
Reinitialized existing Git repository in C:/Users/THANH TOAN/Desktop/1649/.git/

C:\Users\THANH TOAN\Desktop\1649>git add README.md

C:\Users\THANH TOAN\Desktop\1649>git commit -m "first commit"
[main (root-commit) bfdea97] first commit
 1 file changed, 3 insertions(+)
 create mode 100644 README.md

C:\Users\THANH TOAN\Desktop\1649>git branch -M main

C:\Users\THANH TOAN\Desktop\1649>git remote add origin https://github.com/thanhtoan99/toanttgcs200873.git
error: remote origin already exists.

C:\Users\THANH TOAN\Desktop\1649>git push -u origin main
info: please complete authentication in your browser...
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Delta compression using up to 20 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 251 bytes | 251.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
To https://github.com/thanhtoan99/toanttgcs200873.git
 * [new branch]      main -> main
branch 'main' set up to track 'origin/main'.

C:\Users\THANH TOAN\Desktop\1649>git remote add origin https://github.com/thanhtoan99/toanttgcs200873.git
error: remote origin already exists.

C:\Users\THANH TOAN\Desktop\1649>git branch -M main

C:\Users\THANH TOAN\Desktop\1649>git push -u origin main
branch 'main' set up to track 'origin/main'.
Everything up-to-date

C:\Users\THANH TOAN\Desktop\1649>
```

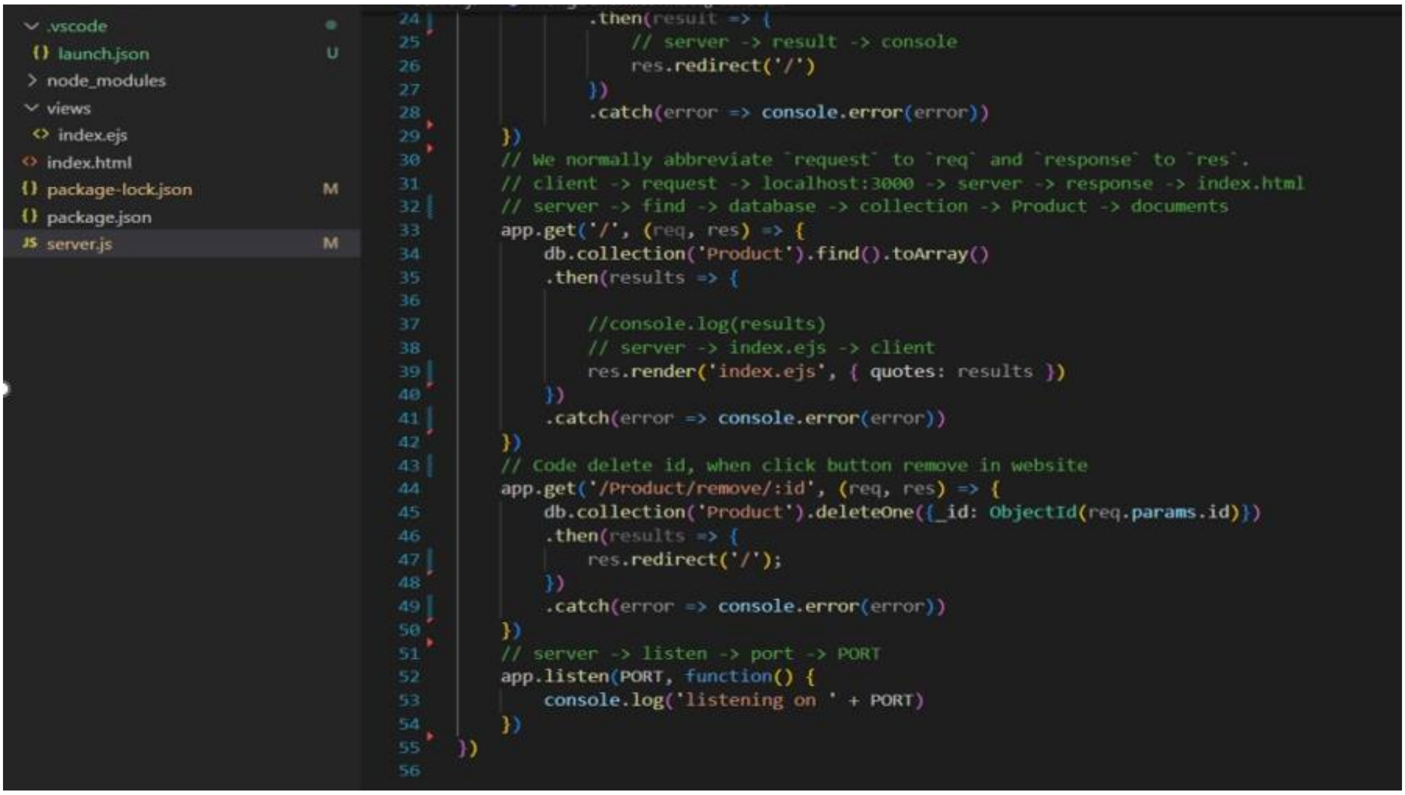
3. Nodejs Push MongoDB.

Note

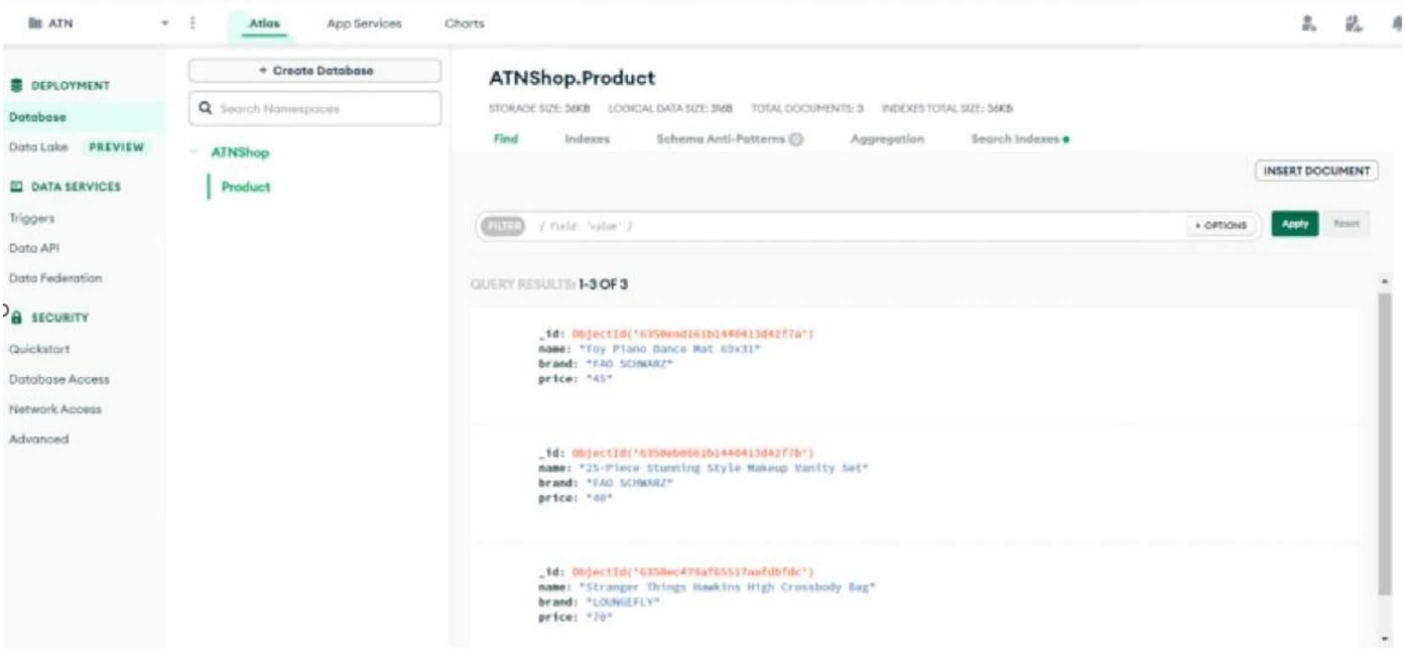
The node .\server.js command creates a database and collection for your data.



```
const express = require('express');
const bodyParser= require('body-parser')
const MongoClient = require('mongodb').MongoClient
const ObjectId = require('mongodb').ObjectId;
const PORT = process.env.PORT || 8080;
const app = express();
// This tells Express we're using EJS as the template engine.
app.set('view engine', 'ejs')
// Make sure you place body-parser before your CRUD handlers!
app.use(bodyParser.urlencoded({ extended: true }))
const connectionString = 'mongodb+srv://locdb:abc123456@cluster13.ynbwogf.mongodb.net/?retryWrites=true&w=majority'
// server -> connect -> MongoDB
MongoClient.connect(connectionString, (err, client) => {
    if (err) return console.error(err)
    console.log('Connected to Database')
    // server -> create -> database -> 'star-wars-quotes'
    const db = client.db('ATNShop')
    // server -> create -> collection -> 'quotes'
    const quotesCollection = db.collection('Product')
    // client -> button -> submit -> request -> post -> '/quotes'
    app.post('/Product', (req, res) => {
        // server -> insert -> data -> from client
        quotesCollection.insertOne(req.body)
            .then(result => {
                // server -> result -> console
                res.redirect('/')
            })
            .catch(error => console.error(error))
    })
    // We normally abbreviate `request` to `req` and `response` to `res`.
    // client -> request -> localhost:3000 -> server -> response -> index.html
    // server -> find -> database -> collection -> quotes -> documents
    app.get('/', (req, res) => {
        db.collection('Product').find().toArray()
        .then(results => {
            //console.log(results)
```



```
            .then(result => {
                // server -> result -> console
                res.redirect('/')
            })
            .catch(error => console.error(error))
    })
    // We normally abbreviate `request` to `req` and `response` to `res`.
    // client -> request -> localhost:3000 -> server -> response -> index.html
    // server -> find -> database -> collection -> Product -> documents
    app.get('/', (req, res) => {
        db.collection('Product').find().toArray()
        .then(results => {

            //console.log(results)
            // server -> index.ejs -> client
            res.render('index.ejs', { quotes: results })
        })
        .catch(error => console.error(error))
    })
    // Code delete id, when click button remove in website
    app.get('/Product/remove/:id', (req, res) => {
        db.collection('Product').deleteOne({_id: ObjectId(req.params.id)})
        .then(results => {
            res.redirect('/');
        })
        .catch(error => console.error(error))
    })
    // server -> listen -> port -> PORT
    app.listen(PORT, function() {
        console.log('listening on ' + PORT)
    })
})
```



```
_id: ObjectId('6350ead161b1440413d42f7a')
name: "Toy Piano Dance Mat 69x31"
brand: "FAO SCHWARZ"
price: "45"
```

```
_id: ObjectId('6350eb0661b1440413d42f7b')
name: "25-Piece Stunning Style Makeup Vanity Set"
brand: "FAO SCHWARZ"
price: "40"
```

```
_id: ObjectId('6350ec479af65517aafdbfdc')
name: "Stranger Things Hawkins High Crossbody Bag"
brand: "LOUNGEFLY"
price: "70"
```

P7. Analyse the most common problems Cloud Computing platform and solutions to these problems.

1. Common Cloud Issues.

The instantaneous delivery of resources such as data and storage on demand is known as cloud computing. With a rapidly increasing market worth, it has demonstrated its innovative nature in the IT business.

Cloud security challenges
Misconfigurations and inadequate change control
Weak control plane
Data breaches
Metastructure and applistructure failures
Abuse and nefarious use of cloud services
Limited cloud usage visibility
Insecure interfaces and APIs
Insider threats
Account hijacking
Insufficient identity, credential, access and key management
Lack of cloud security architecture and strategy

Pic1. Common Cloud Issues.

1.1. Data Security and Privacy.

One of the main concerns when moving to cloud computing is data security. Identity theft, data breaches, malware infections, and many other security problems in the cloud gradually erode consumers' faith in your apps.

Pic2. Data Security and Privacy.

Solution

We ought to equip ourselves with a technique for safeguarding private data. By the way, we have to study up on account protection strategies and cyber security news. As an alternative, we could seek advice on account protection from friends and family members who are knowledgeable about information technology.

1.2. Cost Management.

The hidden costs increase when resources are not optimized, such as when servers are not being used to their maximum capacity. Without even using the resources, the cost will go up if you switch on cloud services or an instance and neglect to turn it off over the weekend or when it's not in use.

Pic3. Cost Management

Solution

In order to minimize the amount of data that is used by the network that is outside of our control, we need proactively set a data traffic restriction.

1.3. Multi-Cloud Environments.

Nearly 84% of these businesses rely on several clouds, and the majority of them employ hybrid cloud strategies. The infrastructure team frequently finds that this is challenging to handle and impedes their progress. Because of the variations across various cloud providers, the procedure frequently ends up being quite difficult for the IT staff.

SIMFORM
Cloud Providers
AWS
Platform
bmc
SCALR
Multi-Cloud Management
Challenges
Best Practices

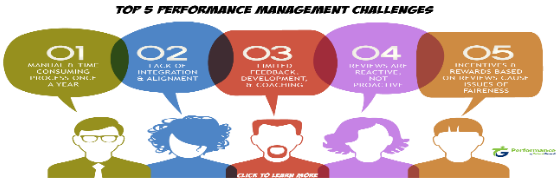
Pic4. Multi-Cloud Environments

Solution

Multi-Cloud Environments ought to be restricted to larger businesses rather than startups. IT staff and time management will decline as a result.

1.4. Performance Challenges.

Inadequate cloud performance has the potential to drive away customers and reduce revenue. A minor delay in the loading of an application or website might cause a significant decrease in the proportion of users. This delay may result from ineffective load balancing, which occurs when the server is unable to divide incoming traffic in a way that optimizes user experience.


TOP 5 PERFORMANCE MANAGEMENT CHALLENGES
01 MANUAL & TIME CONSUMING PROCESS ONCE A YEAR
02 LACK OF INTEGRATION & ALIGNMENT
03 LIMITED FEEDBACK, DEVELOPMENT, & COACHING
04 REVIEWS ARE REACTIVE, NOT PROACTIVE
05 INCENTIVES & REWARDS BASED ON REVIEWS CAUSE ISSUES OF FAIRENESS
CLICK TO LEARN MORE
Performance

Pic5. Performance Challenges

Solution

Users should be split into two groups: those who pay and those who don't. In terms of network connection speed, they will get precedence if they are a paying customer. Those who utilize it for free, on the other hand, will have network connection limitations. In other situations, we ought to boost network storage during high usage and reduce network traffic during off-peak hours. As a result, we will lessen the hardware burden on the network devices.

1.5. Interoperability and Flexibility.

Because of the complexity required, moving between clouds does not offer the same flexibility. The management of data migration, initial security setup, and network configuration further compound the problems that arise when switching cloud solutions, ultimately decreasing flexibility.

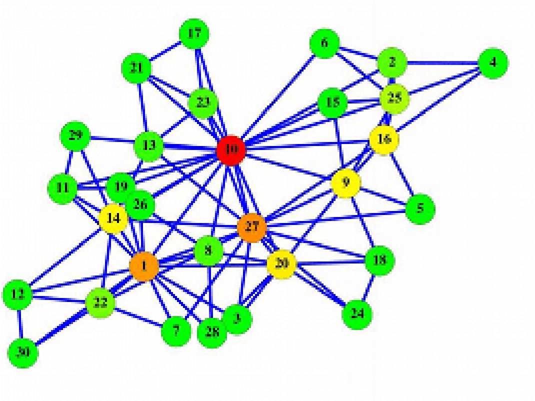
Pic6. Interoperability and Flexibility

Solution

We need to set up separate private clouds for data transport and storage. We will therefore be able to send data over the cloud and lessen the issue of secure data. Prices will increase, but the issue will be resolved.

1.6. High Dependence on Network.

Cloud computing handles massive volumes of data flow to and from the servers as it deals with the real-time supply of resources. Even if these resources and data are transferred across the network, this can be extremely vulnerable in situations when there is a sudden interruption or when bandwidth is restricted.Therefore, maintaining network bandwidth at a high cost is a significant difficulty for smaller businesses.



Pic7. High Dependence on Network

Solution

The number of users connecting to the network should be determined, and then the network speed should be divided by the user's day, month, or time of day. Alternatively, we ought to go with a system that makes advantage of both data transmission and storage clouds. As a result, already produced, saved, and transferred data will move more quickly than freshly created data.

1.7. Lack of Knowledge and Expertise.

It necessitates extensive subject-matter knowledge and proficiency. Even if there are many experts in the industry, they still need to stay up to date. Because of the wide discrepancy between supply and demand, cloud computing is a highly compensated profession. While there are many open positions, there aren't many skilled cloud engineers. Upskilling is therefore required in order for these individuals to actively comprehend, maintain, and create cloud-based applications with the fewest possible problems and the highest possible level of dependability.

Solution

Light chores for humans can be performed by an artificial intelligence that we can construct. Alternatively, we educate a group of youth who possess sufficient understanding about fundamental security. From there, we gave a group of youths the task of protecting the outer layer. Rather, we carry out both.

Pic8. Lack of Knowledge and Expertise

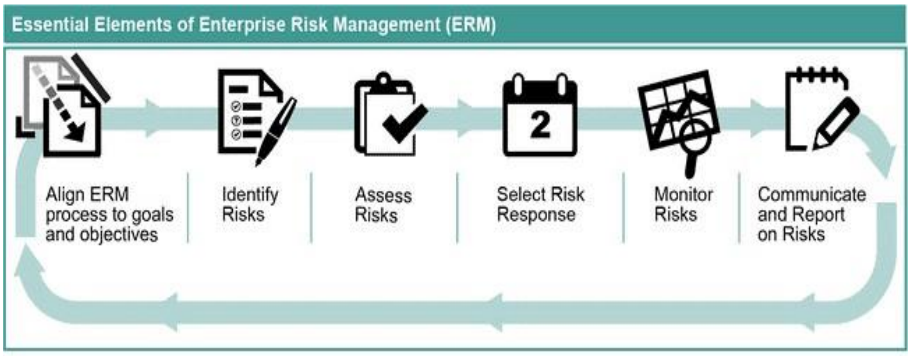
2. Common issues of public, private, hybrid, community.

	Public Cloud	**Private Cloud**	**Community Cloud**	**Hybrid Cloud**
Easy to set up and use	Easy	Knowledge of information technology	Knowledge of information technology	Knowledge of information technology
Data security and privacy	Low	High	Relative high	High
Data is controlled	Medium	High	Relative high	Relative high
Reliability	Low	High	Relative high	High
Extensible and flexible	High	High	Stability	High
Cost	Cheap	Expensive model, expensive cost	Costs are shared with the community	Cheaper than the privatemodel. but more expensive than the public model.
Depending on the hardware	No	Depends on the enterprise	Depends on the enterprise	Depends on the enterprise

3. Security Threats and Vulnerabilities.

As previously stated, we will restrict the scope of our security assessment to the public cloud, which is the most widely used type of cloud. We first outline the fundamental security factors for this deployment paradigm before looking at and classifying the risks unique to CSPs and CSCs.

3.1. Basic Security Risk Considerations


Essential Elements of Enterprise Risk Management (ERM)
Align ERM process to goals and objectives
Identify Risks
Assess Risks
Select Risk Response
Monitor Risks
Communicate and Report on Risks

When it comes to cloud computing, there are several places that might be hacked and therefore need to be guarded. Every space serves as a possible point of failure or assault. Five important such regions have been identified through risk analysis.

Source: GAO. | GAO-17-63

Pic9. Basic Security Risk Considerations

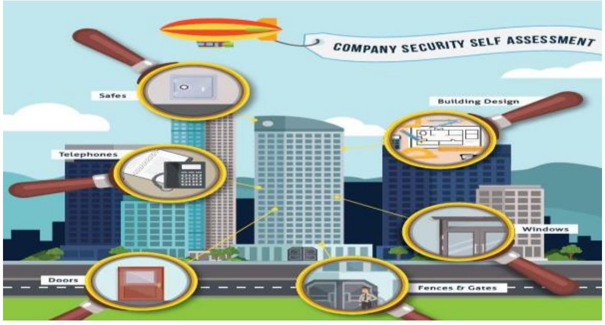
Organizational Security Risks

Organizational risks are defined as those that have the potential to affect an organization's structure or the business as a whole. A CSP's CSPs may suffer if it goes out of business or is bought by another company. This is because any Service Level Agreements (SLAs) it may have had may have altered, and customers would then need to switch to a another CSP that better suits their needs.

Pic10. Organizational Security Risks

Physical Security Risks

An Overview of Security Concerns, Difficulties, and Solutions in Cloud Computing To stop illegal on-site access to CSC data, the cloud data center's physical location has to be guarded by the CSP. Firewalls and encryption are insufficient to prevent physical data theft. Since the CSP is in charge of the physical infrastructure, they should put in place and maintain the necessary infrastructure controls, such as network firewalls, staff training, and physical location security.



Pic11. Physical Security Risks

Technological Security Risks

These hazards include malfunctions related to the CSP's hardware, technology, and services. Among the hazards associated with switching CSPs, or portability, are resource sharing and isolation issues in the public cloud with its multi-tenancy characteristics. It is advised that CSP do routine infrastructure audits and maintenance.

Pic12. Technological Security Risks

Compliance and Audit Risks

These are legal risk factors. That is, the risks associated with incomplete information about jurisdiction, jurisdictional changes, contract provisions that are unlawful, and continuing legal challenges. For instance, depending on their location, certain CSPs can be required by law to provide sensitive data upon request from the government.

Pic13. Compliance and Audit Risks

Data Security Risks

There are several concerns related to data security that we must consider. The three primary attributes that require assurance are availability, confidentiality, and data integrity. We will go deeper into this topic in the next paragraph since the majority of cloud security efforts are directed at this area because it is the most vulnerable to compromise.

Pic14. Data Security Risks

P8 Assess The Most Common Security Issues in Cloud Environments

1. Security Issues

Any unavoidable risk or weakness in your system that hackers may exploit to compromise systems or corrupt data is referred to be a security concern. This includes weaknesses in the people, procedures, and software that run your company and link it to clients, as well as servers and software.

1.1. Ransomware Attack

A ransomware assault aims to take complete control of important data. Your data is encrypted by the hacker, who then keeps it hostage until you pay a ransom for the decryption key that unlocks the contents. If you don't pay by the deadline, the attacker could even obtain sensitive data and threaten to make it publicly available.

Pic15. Ransomware Attack

Solution

Having regular and complete backups of important data stored in a secure location is the best defense against ransomware attacks. A strong backup and recovery strategy reduces the attacker's leverage, enabling you to remove and restore the compromised data.

1.2. Remote Code Execution

An intruder will look for areas inside your application, such a search box, data entry field, or contact form, where users may enter information. The hacker then discovers what different requests and field content will accomplish by trial and error.

Pic16. Remote Code Execution

Solution

Update any framework, content management system, or programming platform frequently with security updates. Observe input sanitization best practices when programming. All user input, regardless of how little, needs to be compared against a fundamental set of guidelines for what constitutes appropriate input.

1.3. Cross-Site Scripting (XSS)

Hackers that use XSS to target your clients typically utilize JavaScript and other browser-side scripting techniques to spread malware or unwanted adverts through your website. As a result, you risk losing the confidence of your customers and damaging your company's brand.

Pic17. Cross-Site Scripting

Solution

Make changes to your content security policy. This simple but frequently missed step can stop a lot of XSS assaults before they ever start. The majority of XSS assaults rely on the site developer's lack of action to stop it. If you are a developer, you may utilize input sanitization to reduce these online security issues by correctly escaping HTML tag characters. For example, you can change < and > to < and > on any user input that JavaScript processes. Taking a few simple precautions can increase safety significantly.

1.4. Data Breach

Anytime an unauthorized person has access to your personal information, there has been a data breach. They may not be able to read or modify the data, but they do have access to a duplicate of it. You might not even be aware right away. For instance, the attacker could already know the password to the administrator account, but they haven't utilized it to make any modifications.

Pic18. Data Breach

Solution

At this point, an attacker is usually taking precautions to stay inconspicuous, which makes addressing this Internet security issue difficult. When you log in, a lot of systems will publish the connection details from your last session. When this information is accessible, take note of it and keep an eye out for unfamiliar activities.

1.5. Malware and Virus Infection

On a workstation, malware can track keystrokes to get passwords or encrypt data for ransomware purposes. Malware is often used by hackers to increase access to your website or provide access to others on the same network.

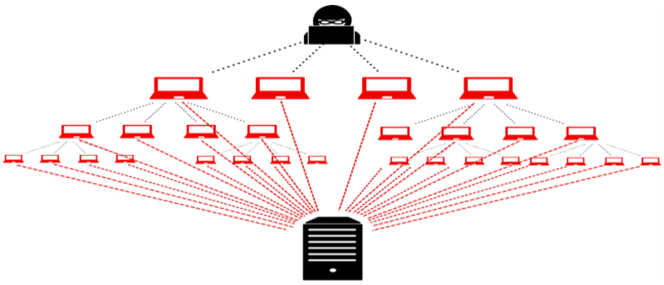
Pic19. Malware and Virus Infection

Solution

Reduce the possibility of this security issue on workstations and personal devices by being cautious about what you download and by using antivirus software to detect and properly delete any malware. It's important to update these antivirus programs on a regular basis since malware is always evolving and getting better.

1.6. DDoS Attack

DoS (denial of service) attacks have a subclass known as distributed denial of service (DDoS) attacks. A distributed denial of service (DDoS) attack uses a network of interconnected computers, or "botnet," to flood a target website with fictitious traffic.



Pic20. DDoS Attack

Solution

The best defenses take all the traffic and absorb it by scaling up server and network resources to handle the extra load until the assault abates or can be contained.

2. Solution for public, private, hybrid, community 's cloud issues

2.1. Solution for Public

Intel-Driven Public Cloud Solutions Certain workloads are more appropriate for private infrastructure, while others are better suited for the public cloud. A hybrid, multicloud strategy will yield the greatest benefits for the majority of enterprises. In order to guarantee that you may utilize your desired combination of public and private cloud resources, Intel collaborates with ecosystem partners including VMWare - Intel Virtualize ASAP, Red Hat, and Microsoft in addition to leading cloud service providers (CSPs) like AWS, Google Cloud, and Microsoft Azure.

2.2. Solution for Private

Internal cloud, often known as private cloud, is a pre-installed system. It allows access to customer-specific resources, such as software and hardware. The firewall-protected system and the enterprise itself are the primary means of managing the model.

2.3. Solution for Hybrid

The answer to separating cloud infrastructure and data center transition is hybrid cloud. The Public Cloud, which is powered by Google Cloud, AWS, and cloud services combined on a single management engine, is then connected to this cloud architecture. From then, companies use a central control to assign, oversee, and manage resources.

2.4. Solution for Community

Because Community Cloud is adaptable and extendable, it works well for most users. Clients may personalize computers and smart mobile devices to suit their needs. therefore cutting expenses and the need for workers to interact remotely with clients. Lastly, Community Cloud guarantees trust and data security.

3. Methods to Ensure Security in the cloud

Now that the several concerns associated with cloud computing have been discussed, let's look at the solutions the industry has created to address these problems. In addition to briefly examining the tactics utilized to address the other secondary concerns, this part will concentrate on the techniques utilized to guarantee the distinct types of data security.

3.1. Countermeasures for Security Risks

We provide a brief summary of the several methods that are applied in the industry to secure specific problems in these domains.

Pic21. Countermeasures for Security Risks

Organizational Security Risks

Malicious Insiders: Strict legal requirements should be included in employment contracts to reduce the possibility of having hostile employees within a CSP's workforce. Preventing this may also be greatly aided by a thorough third-party evaluation of the CSP and a strong security breach reporting procedure.

Physical Security Risks

Physical Breach: Having robust physical security measures in place, such as armed guards, keycard access, and biometric scans to restrict access to sensitive locations in the data center, can help lower the risk of hackers physically accessing devices used in the provision of cloud services.

Technological Security Risks

Virtualized defense and reputation-based trust management: CSP may employ a hierarchy of DHT-based overlay networks, with each layer responsible for carrying out particular functions. The lowest layer looks at colluders and handles reputation aggregation. The topmost layer handles several types of assaults. Interoperability and security through a trust model: Providers and users should have their own domains, each with a unique trust agent.

Compliance and Audit Risks

Since this field mostly deals with legal matters, it is important for CSPs and CSCs to be aware of their legal and regulatory responsibilities and to make sure that any contracts they enter into comply with them. Additionally, the CSP needs to make sure that data security and privacy are not jeopardized by its discovery capabilities.

References

1. Viettelidc.com.vn (no date) Công Ty Tnhh Viettel - cht, viettelidc.com.vn. Available at: https://viettelidc.com.vn/tin-tuc/cam-nang-cloud-tong-hop-kien-thuc-ve-dam-may-cong-dong- community-cloud (Accessed: 1 March 2024).

2. Triển Khai MÔ Hình điện Toán đám Mây Lai Hybrid Cloud (2022) Tổng công ty Công nghệ và Giải pháp CMC. Available at: https://cmcts.com.vn/vi/dam-may-lai-hybrid-cloud.html (Accessed: 1 March 2024).

3. (SỐ 1) Giải Pháp xây dựng private cloud Cho Doanh Nghiệp: CMCTS.com. (2022) Tổng công ty Công nghệ và Giải pháp CMC. Available at: https://cmcts.com.vn/vi/giai-phap-private-cloud.html (Accessed1 March 2024).

4. Buy stranger things hawkins high crossbody bag at Loungefly. (no date) Loungefly US. Available at: https://loungefly.com/stranger-things-hawkins-high-crossbody-bag/NFXTB0045.html (Accessed: 1 March 2024).

5. LiquidWeb (no date) The 15 top critical security threats and how to fix them, Liquid Web. Available at: https://www.liquidweb.com/blog/most-common-web-security-problems/#:~:text=A%20security%20issue%20is%20any,your%20business%20processes%20and%20 people.. (Accessed: 1 March 2024).

6. Calzon, B. (2023) Learn the top cloud computing challenges, risks & issues, datapine. Available at: https://www.datapine.com/blog/cloud-computing-risks-and-challenges. (Accessed: 1 March 2024).

7. Elom Worlanyo, A Survey of Cloud Computing Security, Security.pdf, 2013 Default. 2023. What Is PaaS - Advantages and Disadvantages | Cloud Computing | CompTIA . [ONLINE] Available

at: https://www.comptia.org/content/articles/what-is-paas. (Accessed: 1 March 2024).

8. Elom Worlanyo, A Survey of Cloud Computing Security, Security.pdf, 2013 Default. 2023. What Is PaaS - Advantages and Disadvantages | Cloud Computing | CompTIA . [ONLINE] Available

at: https://www.comptia.org/content/articles/what-is-paas. (Accessed: 1 March 2024).

9. Elom Worlanyo, A Survey of Cloud Computing Security, Security.pdf, 2013 Default. 2023. What Is PaaS - Advantages and Disadvantages | Cloud Computing | CompTIA . [ONLINE] Available

at: https://www.comptia.org/content/articles/what-is-paas. (Accessed: 1 March 2024).

10. Elom Worlanyo, A Survey of Cloud Computing Security, Security.pdf, 2013 Default. 2023. What Is PaaS - Advantages and Disadvantages | Cloud Computing | CompTIA . [ONLINE] Available

at: https://www.comptia.org/content/articles/what-is-paas. (Accessed: 1 March 2024).

Image link:

Top 11 cloud security challenges and how to combat them | TechTarget

Data Security vs Data Privacy - TermsFeed

https://www.pinterest.com/pin/505036545687494112/

https://www.google.com.vn/url?sa=i&url=https%3A%2F%2Frhapsody.health%2Fblog%2Finteroperability-the-current-state-of-the-future%2F&psig=AOvVaw0DTmny4elKsFAZRKMNczZw&ust=1709268841054000&source=images&cd=vfe&opi=89978449&ved=0CBMQjRxqFwoTCNi4xePgz4QDFQAAAAAdAAAAABAD

https://www.researchgate.net/publication/223551759/figure/fig12/AS:667069968302087@1536053282669/a-Correlation-and-b-dependency-network-of-all-components-of-the-DJIA-for-the-full.ppm

https://www.checkpoint.com/de/support-services/cyber-security-risk-assessment/

https://www.smartdatacollective.com/key-challenges-companies-face-with-big-data-security/

https://empmonitor.com/blog/data-security-cybersecurity-to-look-out-for/