UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

Contents

Introduction: 2

I. ATN 3

1. Instruction 3

a. Functions implemented 3

b. Implement 4

2. ATN website code 6

II. Configure and implement solution for ATN company 8

1. Configure GitHub Desktop: 9

2. Create Application in Heroku 11

3. Upload and deploy code to build website 14

4. Connect to MongoDB 16

III. Common problems 25

References 31

Figure 1: The first interface of the website 5
Figure 2: second interface of ATN's toy sales site 5
Figure 3: GitHub desktop manage source code 6
Figure 4:Step push code to GitHub 7
Figure 5: Link Heroku of website after push code to GitHub and deploy Branch 7
Figure 6: Source code with file CSS 8
Figure 7 Add new Customer code .....
8 Figure 8 Delete Customer code .....
9 Figure 9: code of file app.js .....
10 Figure 10: GitHub Desktop. ..... 10 Figure 11: The first way to create new repository ..... 11 Figure 12 The second way to create new repository ..... 11 Figure 13 Create new repository interface ..... 12 Figure 14 New button

to create new app in Heroku ..... 12 Figure 15 Create new app window in Heroku ..... 13 Figure 16 setting heroku ..... 14 Figure 17 config Heroku with language NodeJS ..... 14 Figure 18 source code and GitHub desktop after push 15
Figure 19 code after change and push origin in GitHub desktop 15
Figure 20 Deploy the code in Heroku 16
Figure 21 View button in Heroku 17
Figure 22 interface of MongoDB Atlas 17
Figure 23 Access database and new database User 18
Figure 24 Create user and password 19
Figure 25 after Create user and password 19
Figure 26 add new IP Address 19
Figure 27 config IP 20
Figure 28 Build a Cluster 20
Figure 29 Create a cluster 21
Figure 30 connect Cluster0 21
Figure 31 choose connect using MongoDB compass 22
Figure 32 link to MongoDB 23
Figure 33 MongoDB in Desktop 24
Figure 34 data after Create 24
Figure 35 Data after insert 25
Figure 36 source code and step insert data 26
Figure 37 Cloud provider risk categories 29
Figure 38 Information security component..... 31

Introduction:

Cloud computing applications are trendy in companies and organizations, but there are many problems and risks in this technology too. This article also shows how to deploy the website of the ATN company based on the cloud platform and some binding issues in the implementation process to give a small example for deploying a website based on cloud computing. This article also discusses the most common issues that arise in the cloud computing platform, as well as the appropriate solutions to these issues. In addition, the most common security problems in a cloud setting are also addressed, and how to solve them.

I. ATN

ATN 's website was built based on the PaaS model and the Community cloud.

1. Instruction

a. Functions implemented

The ATN Website has 2 parts:

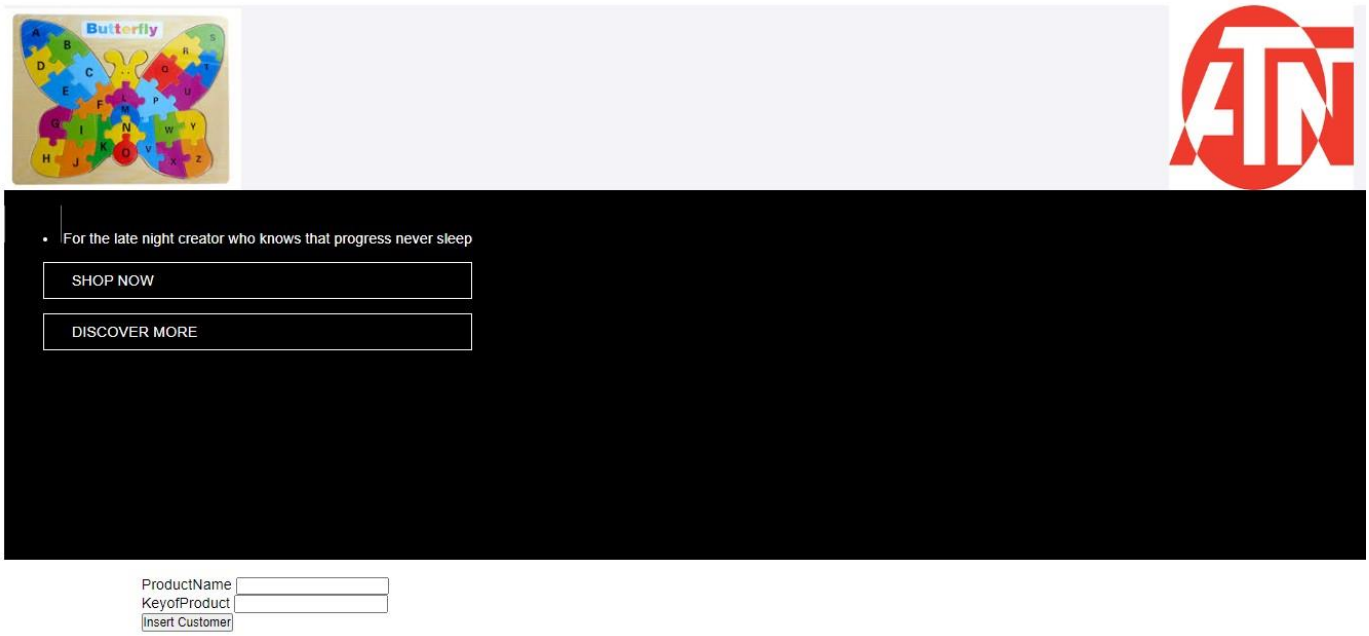

Figure 1: The first interface of the website

First page is web site for employees to add products, if the employee enters the product name and product prefix and presses the insert button, the result will be displayed on the next page of the website.

Figure 2: second interface of ATN's toy sales site

b. Implement

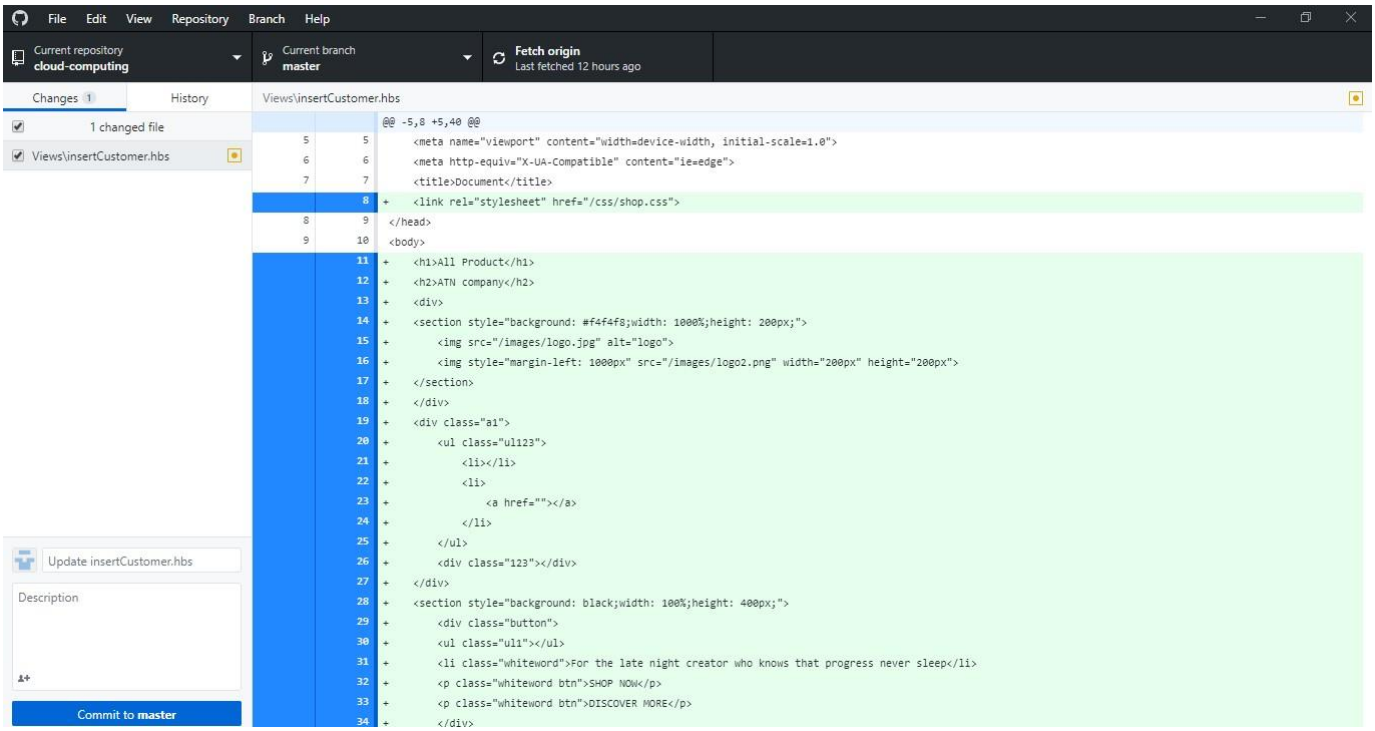

Figure 3: GitHub desktop manage source code

GitHub is used to manage source code:

```
PS E:\copy 3-4-2019\Desktop\1644\Assignemnt Set 2- update Oct2019\Demo\MVCApp\cloud-computing> npm install express handlebars consolidate
```

As mentioned in assignment 1, Visual Studio Code is the IDE used for the development. Consolidate module was built for the coding in this IDE, express and handlebars

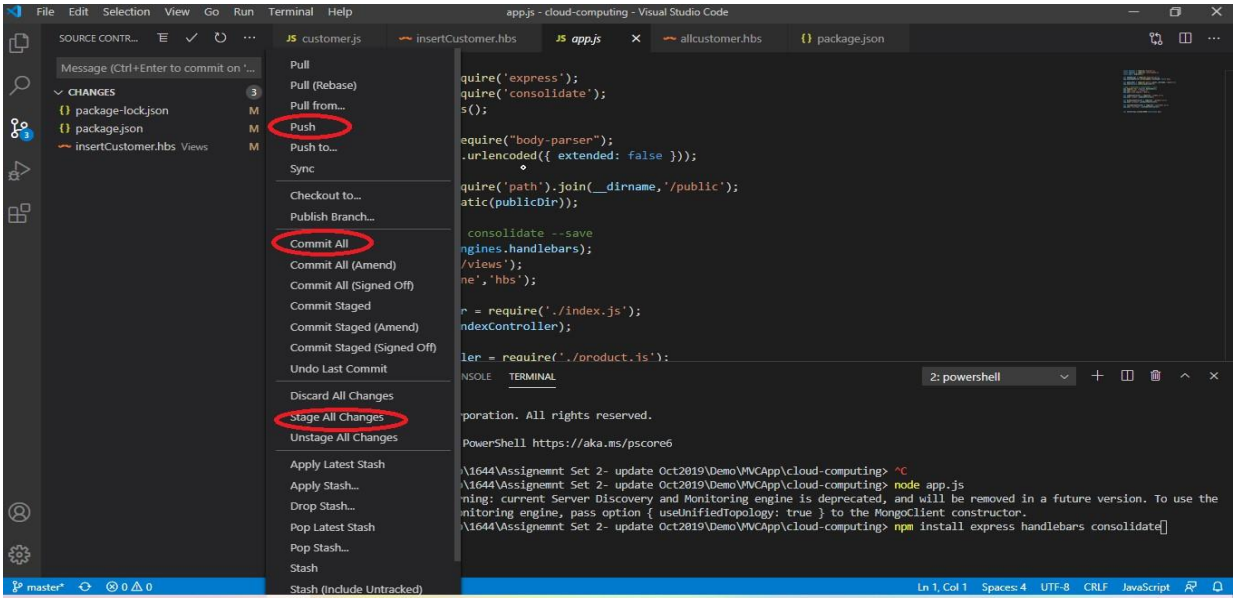

Figure 4:Step push code to GitHub

There are 3 steps to push code to GitHub: Stage all changes => commit all => push.

```
PS E:\copy 3-4-2019\Desktop\1644\Assignemnt Set 2- update Oct2019\Demo\MVCApp\cloud-computing> npm init
```

To make the code can deploy on Heroku web server, the code need file packet.json.

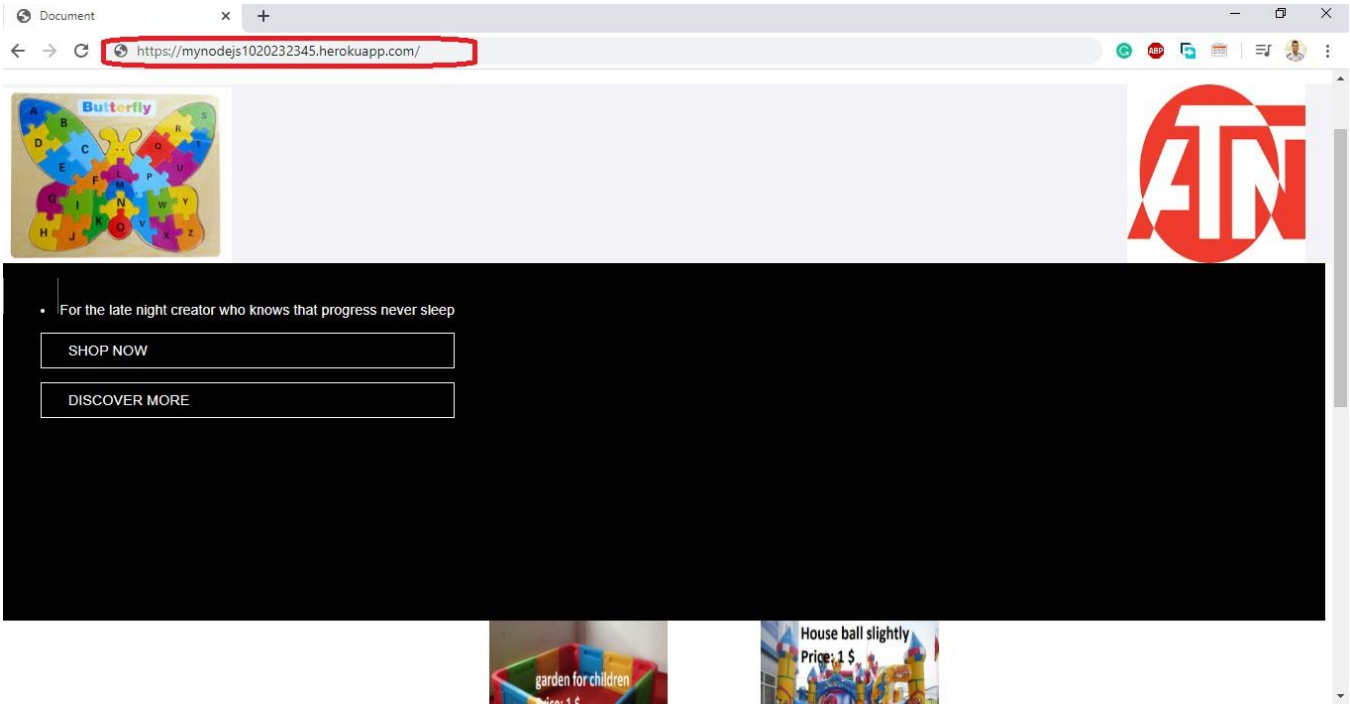

Figure 5: Link Heroku of website after push code to GitHub and deploy Branch

Lastly, developers simply need to create a new Heroku app, connect to GitHub and deploy the brand.

2. ATN website code

Admin website for ATN company has some basic features: login, display all products, add Customers, delete information customer

Add new product function: when the employee types the customer name and clicks on "Insert Customer" at the bottom of the screen on the product display page, they will be redirected to the part 2nd product page. Here, employees enter the information of the product and click the Insert button to save the product, click the Delete button to delete all information.

Figure 6: Source code with file CSS

```
form action="doInsert" method="post">
   Name <input type="text" name="txtName" id="">
   <br>
   Address <input type="text" name="txtAddress" id="">
   <br>
   <input type="submit" value="Insert Customer">
/form>
```

```
<table border="1">
    <tr>
        <td>Name</td>
        <td>Address</td>
        <td>function</td>
    </tr>
    {{#each customers}}
        <tr>
            <td>{{name}}</td>
            <td>{{address}}</td>
            <td><a href="/customer/delete?id={{_id}}">Delete</a></Td>
        </tr>
    {{/each}}
</table>
```

```
    await dbo.collection("customers").deleteOne(condition);
    //
    let results = await dbo.collection("customers").find({}).toArray();
    res.render('allCustomer',{customers:results});
})

router.post('/doInsert',async (req,res)=>{
    let client= await MongoClient.connect(url);
    let dbo = client.db("MyDb");
    let nameValue = req.body.txtName;
    let addressValue = req.body.txtAddress;
    let newCustomer = {name : nameValue, address:addressValue};
    await dbo.collection("customers").insertOne(newCustomer);

    let results = await dbo.collection("customers").find({}).toArray();
    res.render('allCustomer',{customers:results});
```

Figure 7 Add new Customer code

Delete function: when the employee entered the customer name, the Delete button in the rightmost column displaying the Customer information, the Customer is deleted

```
{{#each customers}}
    <tr>
        <td>{{name}}</td>
        <td>{{address}}</td>
        <td><a href="/customer/delete?id={{_id}}">Delete</a></Td>
    </tr>
{{/each}}
```

Figure 8 Delete Customer code

You can access ATN website via the following link:
https://mynodejs1231958.herokuapp.com/customer/insert?fbclid=IwAR1gYRCX097DQW-UYbftKvwv3XYF2d9HrmOiVoN90WvjublzzqSw2x6TY4s

The code for this website is in the link: https://github.com/kenalexander103/demo5.git

```
JS app.js > ...
1   const express = require('express');
2   const engines = require('consolidate');
3   const app = express();
4
5   var port = process.env.PORT || 5000;
6   var bodyParser = require("body-parser");
7   app.use(bodyParser.urlencoded({ extended: false }));
8
9   var publicDir = require('path').join(__dirname,'/public');
10  app.use(express.static(publicDir));
11
12  //npm i handlebars consolidate --save
13  app.engine('hbs',engines.handlebars);
14  app.set('views','./views');
15  app.set('view engine','hbs');
16
17  var indexController = require('./index.js');
18  app.use('/',indexController);
19
20  var productController = require('./product.js');
21  app.use('/product',productController);
22
23  var customerController = require('./customer.js');
24  app.use('/customer',customerController);
25
26
27  var server=app.listen(port,function() {});
```

Figure 9: code of file app.js

Line 1,2: command to run express module.

Line 26: the web can be access on port 5000.

Line 8,9: link files in public folder to file.app.

Line 12 to 23: connect to index page and about page.

II. Configure and implement solution for ATN company

As stated in the previous plan, ATN's cloud solutions will include Visual Studio Code 3 to the NodeJS file code, mongodb NoSQL booster, mongodb compass community, GitHub Desktop as Applications, and Heroku as cloud platform. Here are the steps to create a cloud-based website with some basic features that illustrate the cloud services being deployed for ATN.

1. **Configure GitHub Desktop:**

You need to do the following for using the GitHub desktop:

Use the link to access the GitHub home page: https:/github.com/ and to register an account. Users need to enter a username, password, and email address to open an account. Users need to access the registered email account after clicking on Sign up to activate the account.

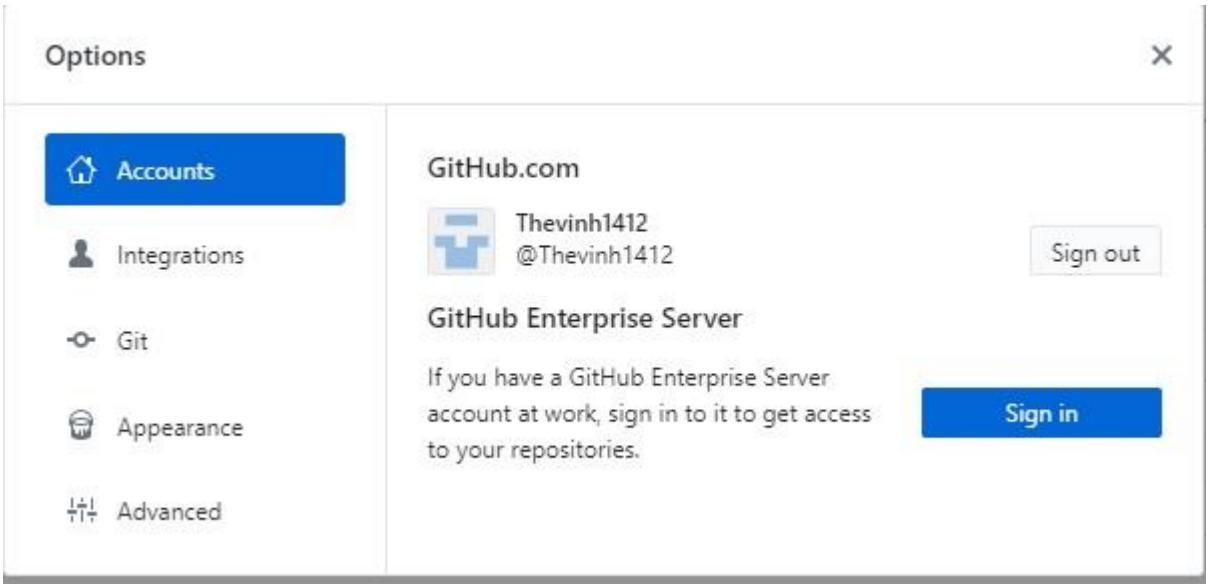

Figure 10: GitHub Desktop.

Users can create a repository on the GitHub homepage after registration or download GitHub desktop to the link: https:/desktop.github.com/ and then add a user with the registered account after installing GitHub Desktop.

- A repository is created in two ways. The first: click File, click New repository, the second: click the arrow to the left of the repository, click Add, click Create a new repository

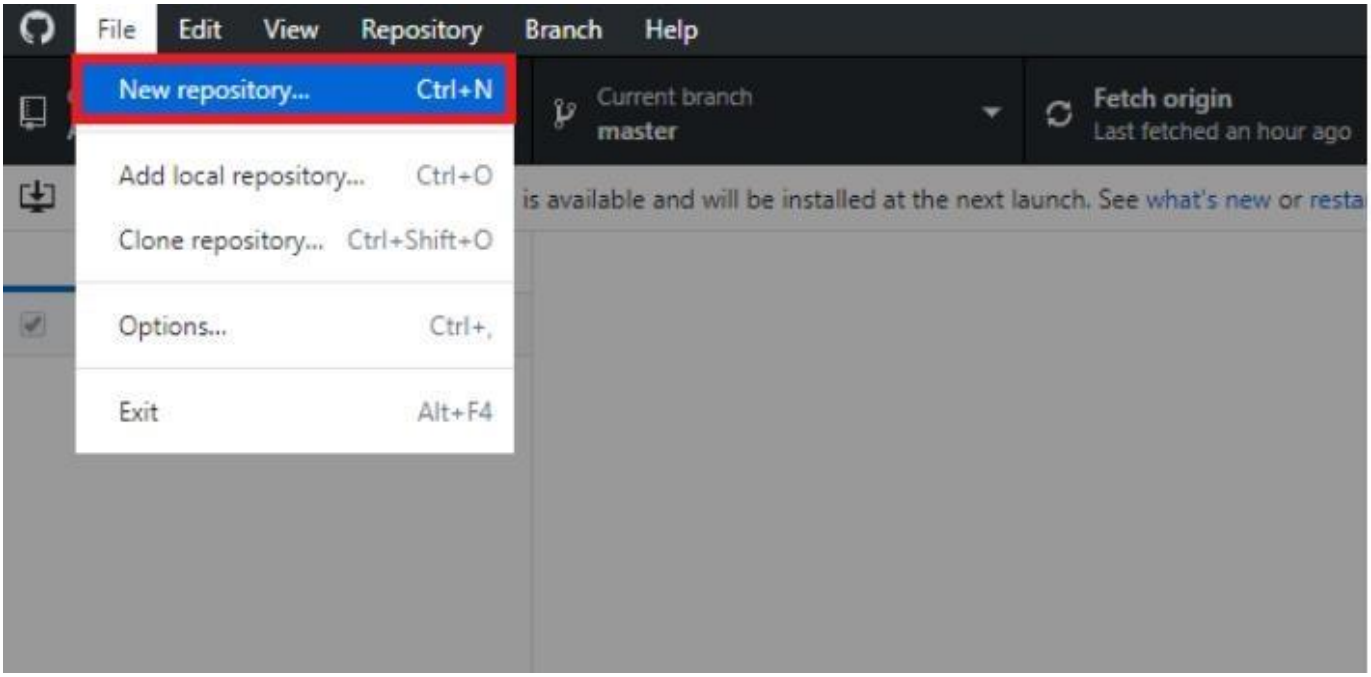

Figure 11: The first way to create new repository

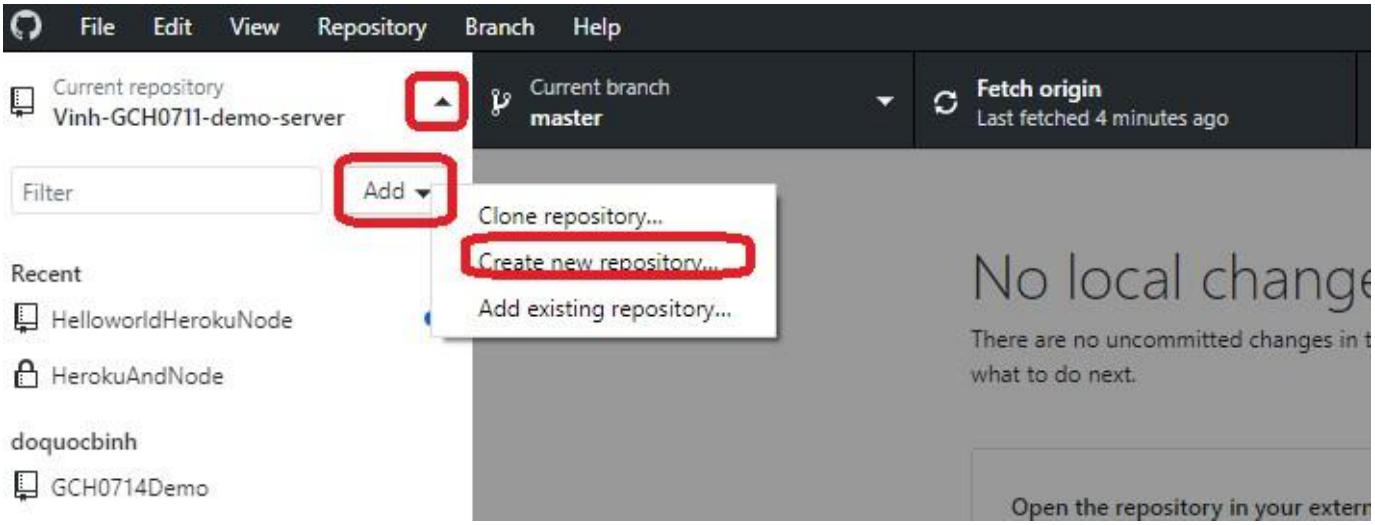

Figure 12 The second way to create new repository

Enter the repository name, and select the location of the file. Then, press the "Build File" button to create a new file.

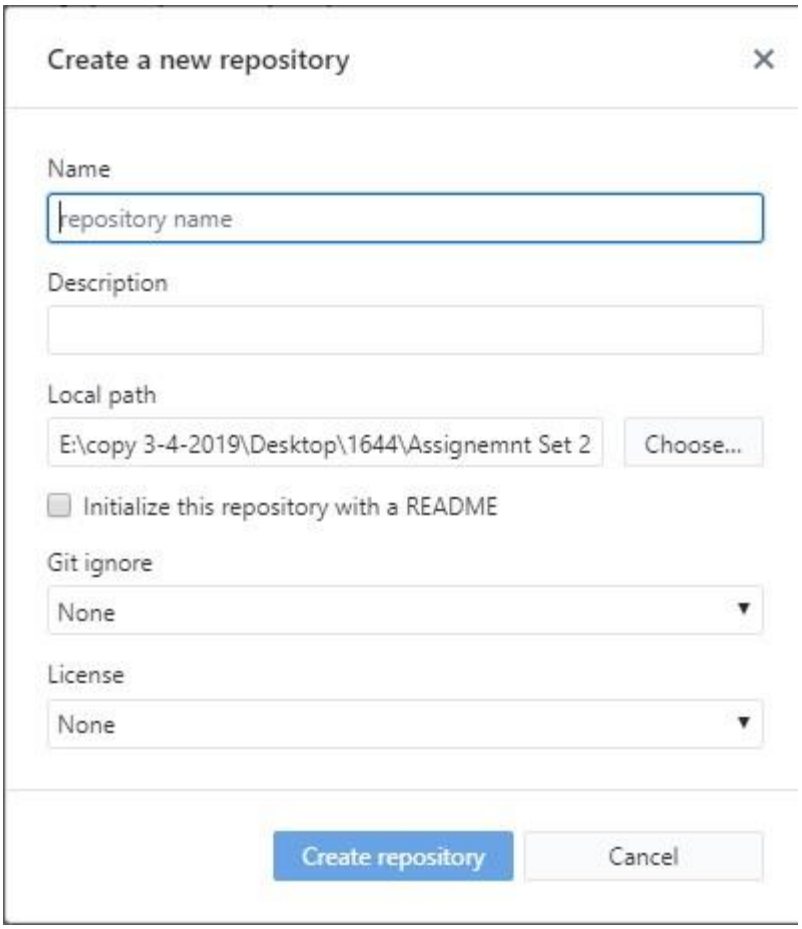

Figure 13 Create new repository interface

2. Create Application in Heroku

Connect to Heroku by following the link: https:/www.heroku.com/ and clicking the Sign-Up button to register for a Heroku account. Then follow all their to sign up guides.

Click on the New button in the top right corner to create a new application after you sign up. User type their device name in the Create New App window, and then press Create App button.

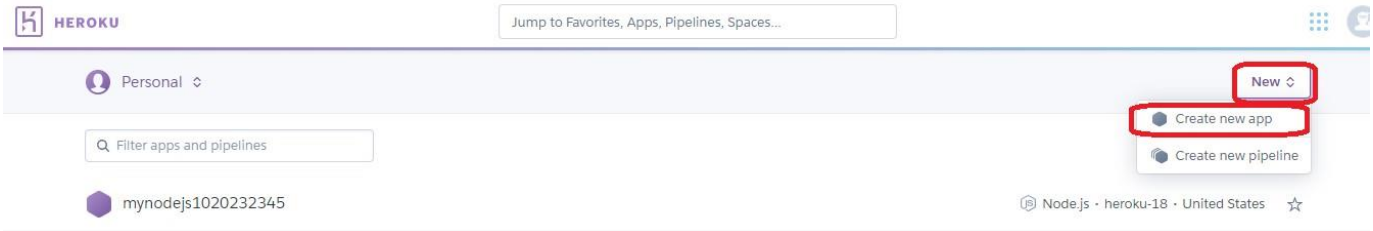

Figure 14 New button to create new app in Heroku

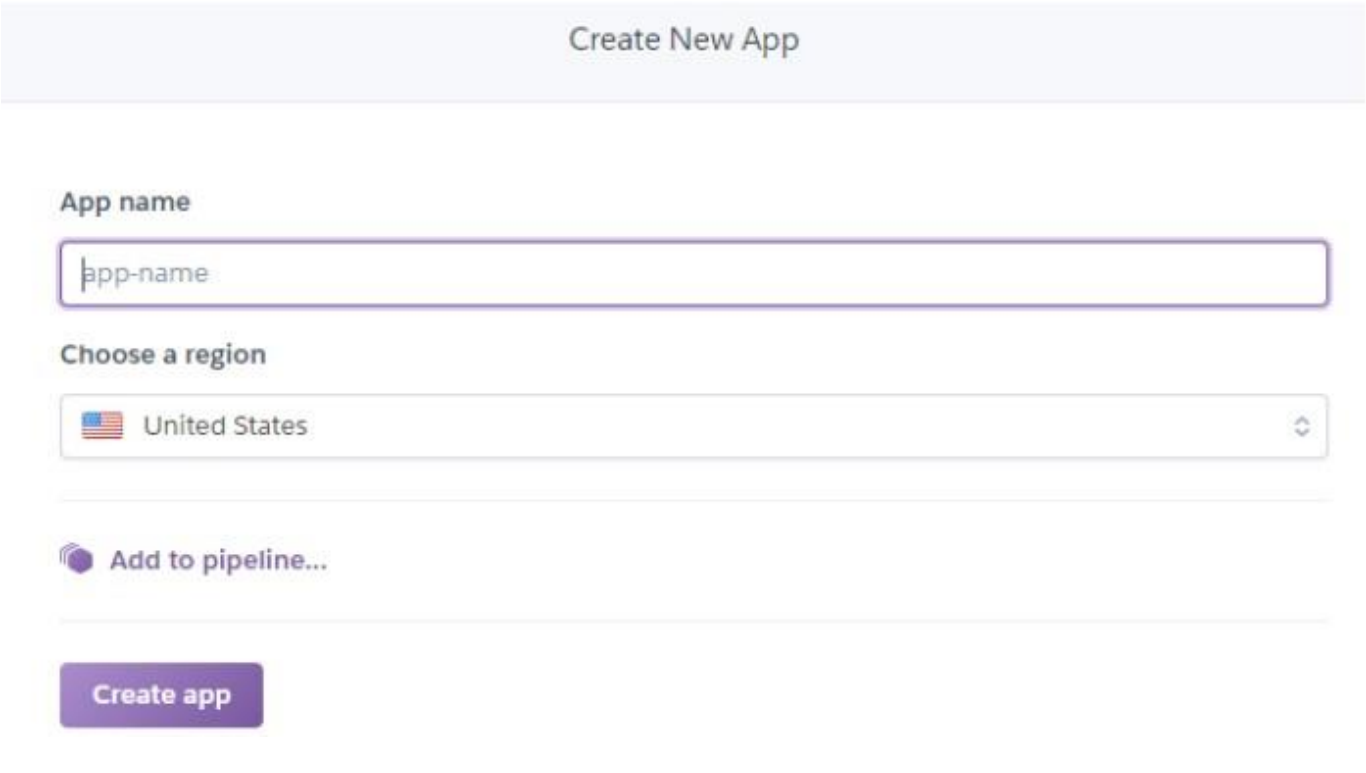

Figure 15 Create new app window in Heroku

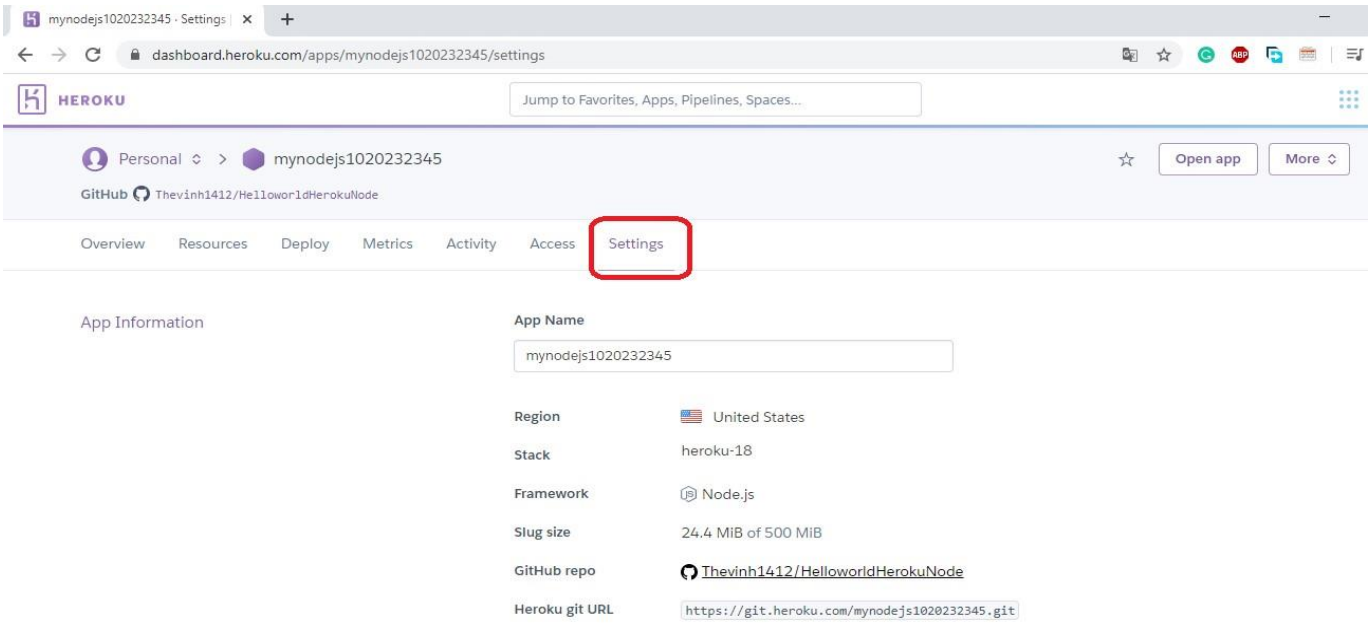

Figure 16 setting heroku

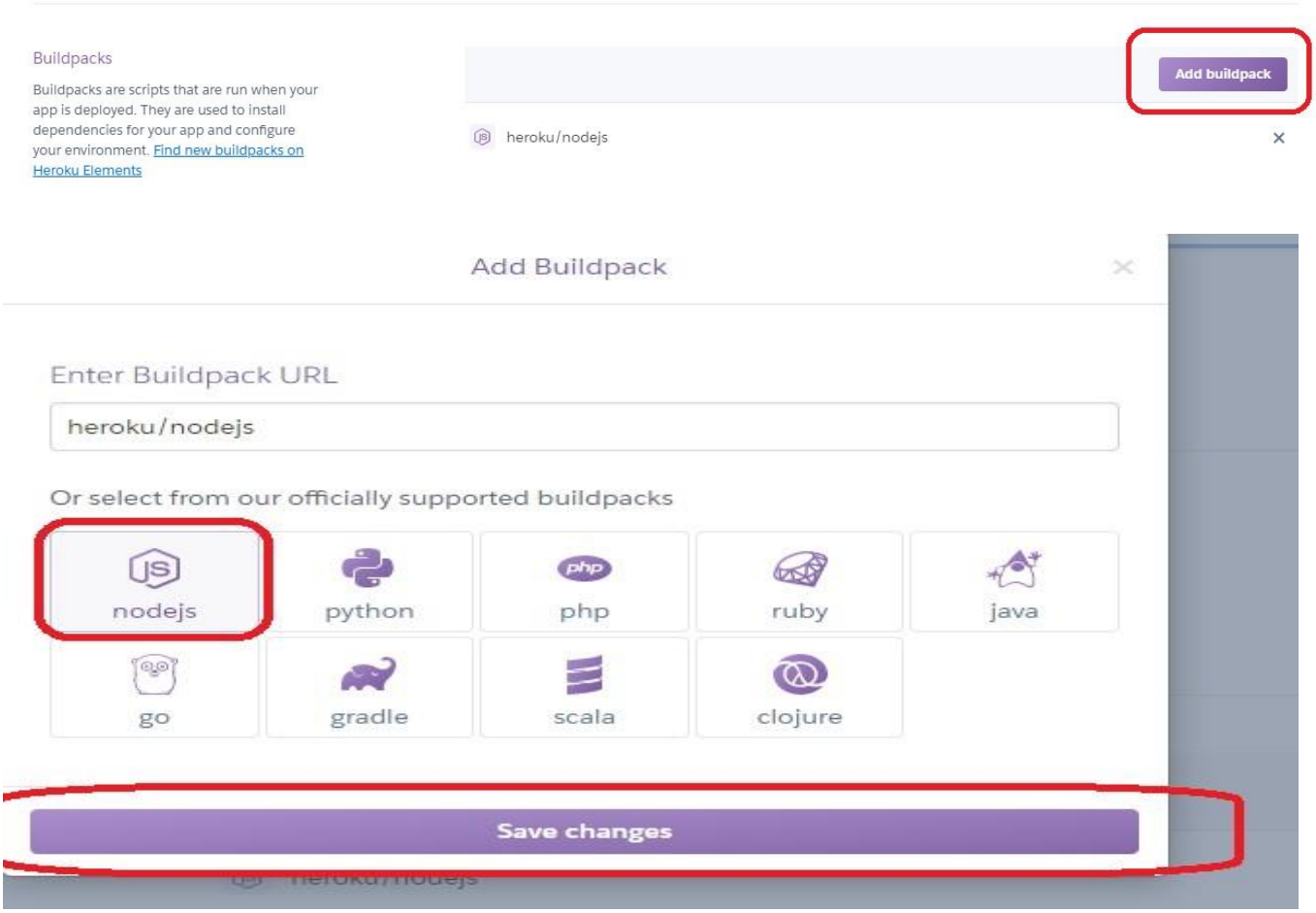

Figure 17 config Heroku with language NodeJS

After creating the application name, the interface will be displayed as the image below and click on settings, select add buildpack and then select nodejs and click on save changes

3. Upload and deploy code to build website

To view the location of this repository, open GitHub Desktop -> click Repository -> click Show in Explorer.

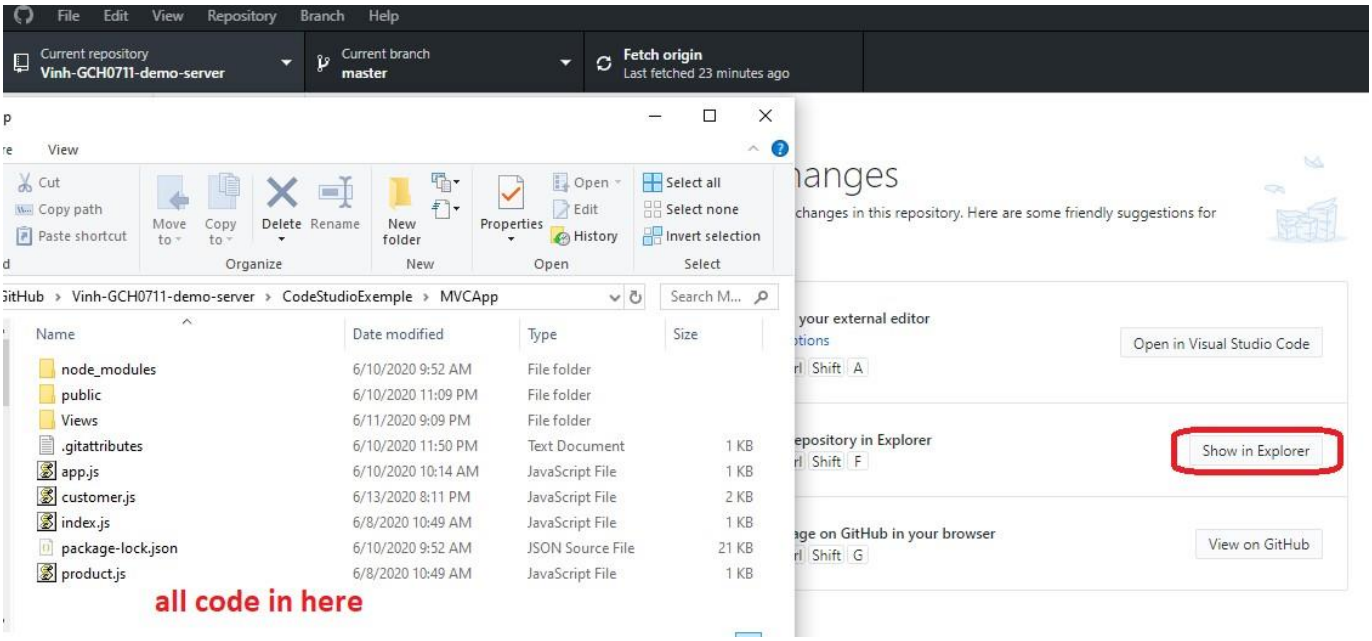

Figure 18 source code and GitHub desktop after push

Click to Push origin to upload code and wait a bit time for the process

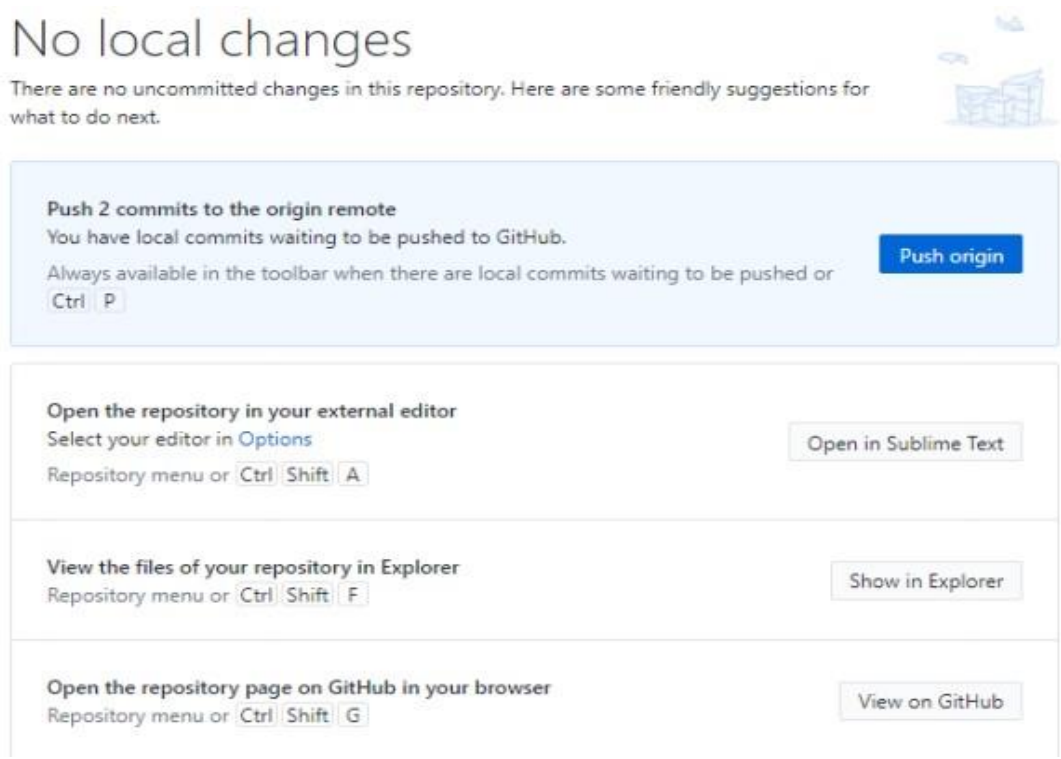

Figure 19 code after change and push origin in GitHub desktop

Open your Heroku app project and click the Deploy button, then scroll down the web to the last one, click the Deploy Branch button to deploy code to your Heroku app, and click the View button to visit the app.

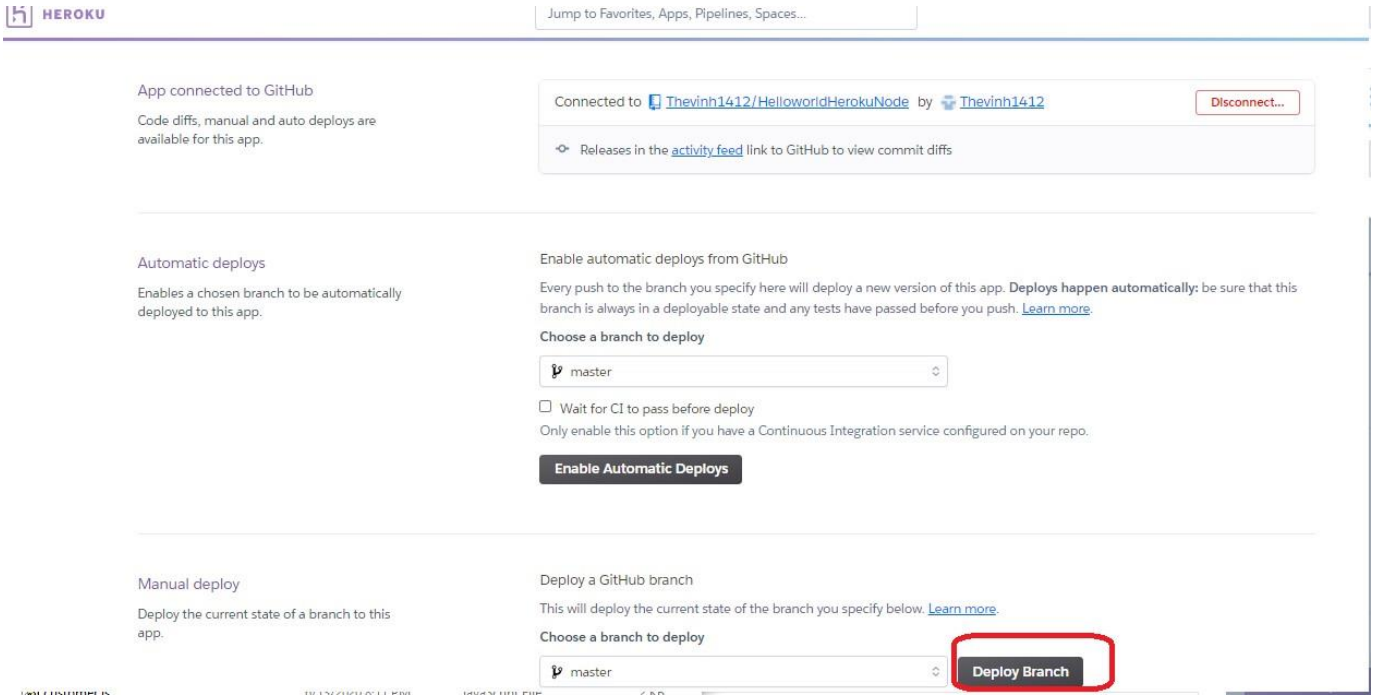

Figure 20 Deploy the code in Heroku

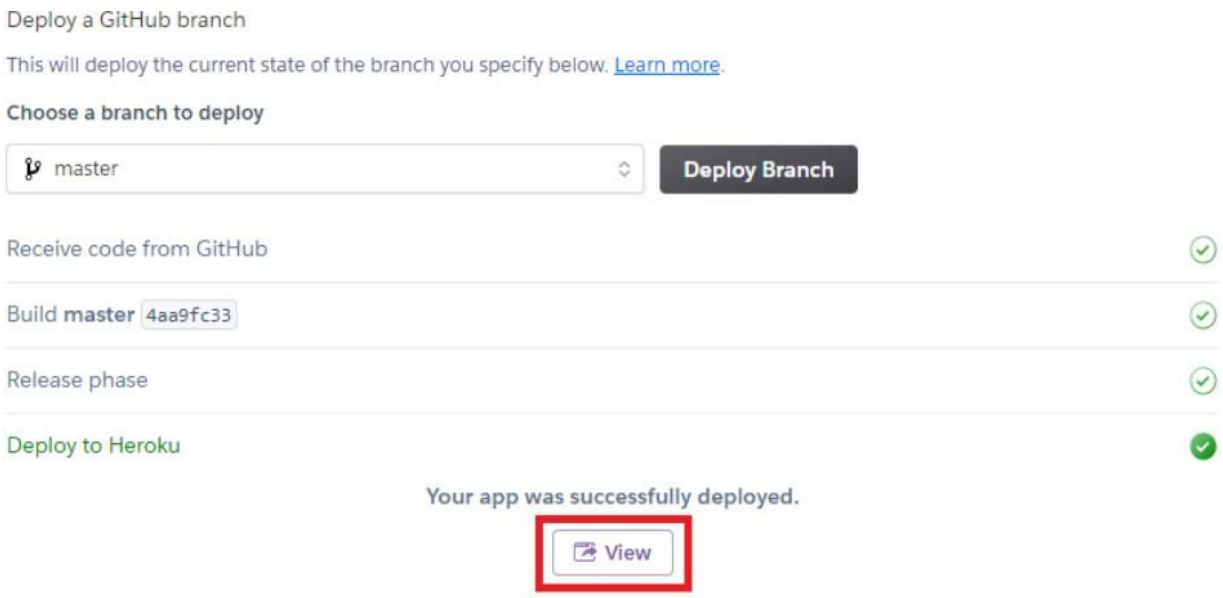

Figure 21 View button in Heroku

4. Connect to MongoDB

- To connect the website to MongoDB we need to config and perform steps:

- access the link: https://www.mongodb.com/cloud/atlas and then press login with gmail

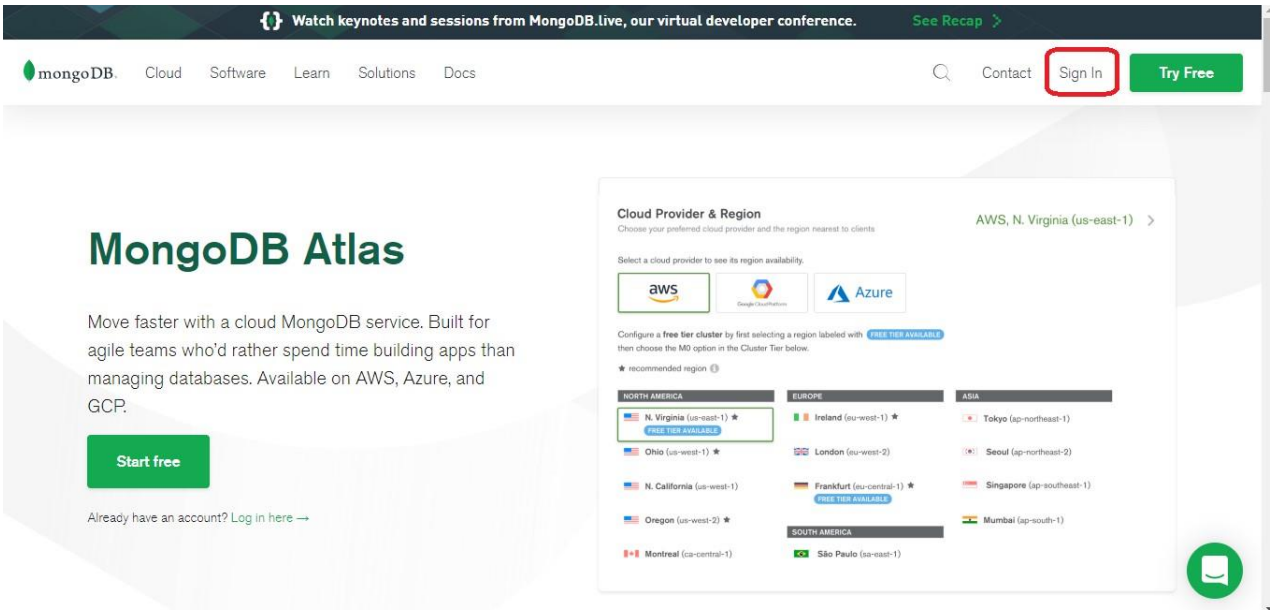

Figure 22 interface of MongoDB Atlas

After sign in click database access and then click button Add New Database User create password and user.

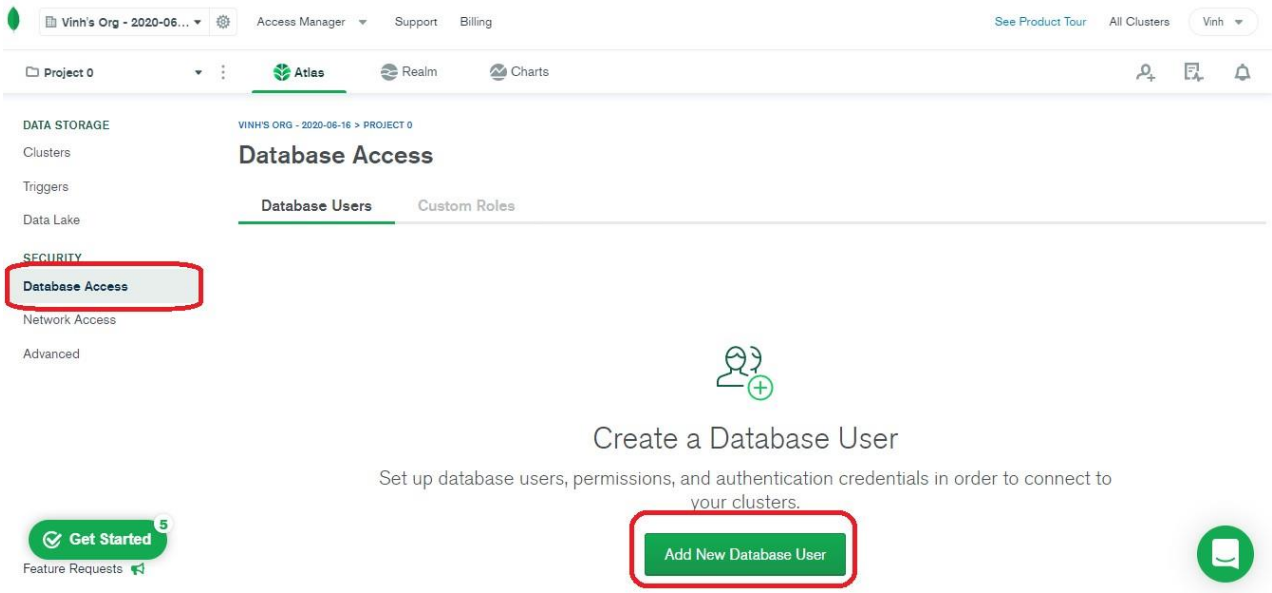

Figure 23 Access database and new database User

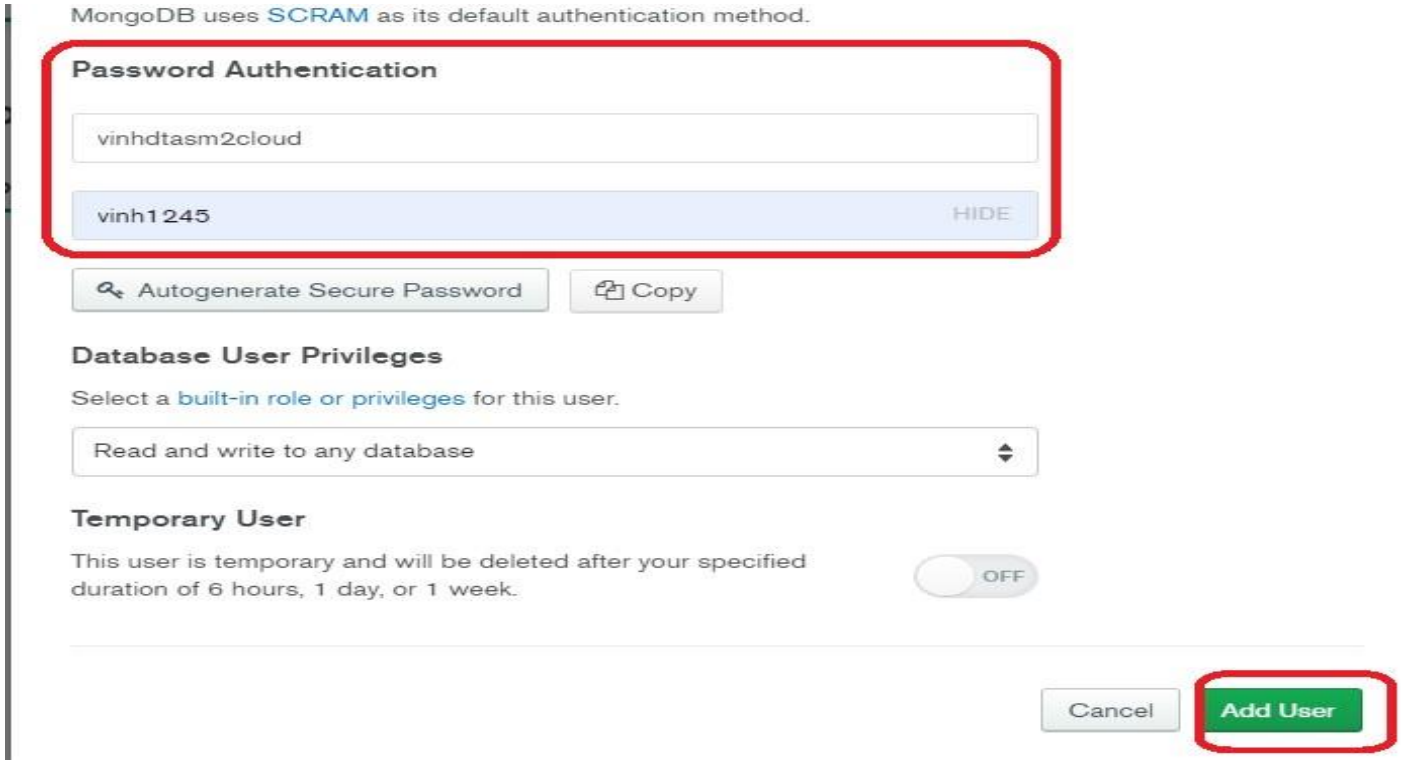

Figure 24 Create user and password

Figure 25 after Create user and password

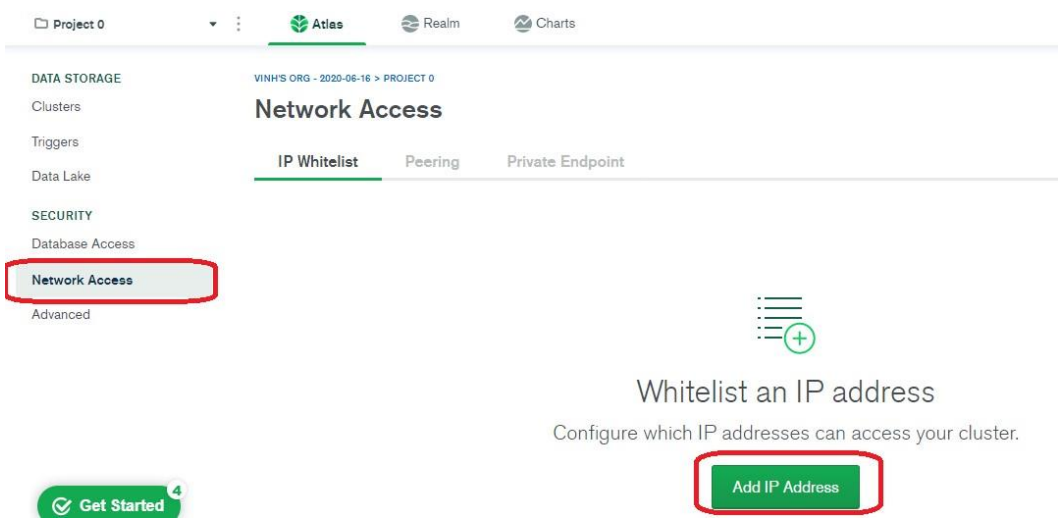

Figure 26 add new IP Address

Here is user Name and password have been created

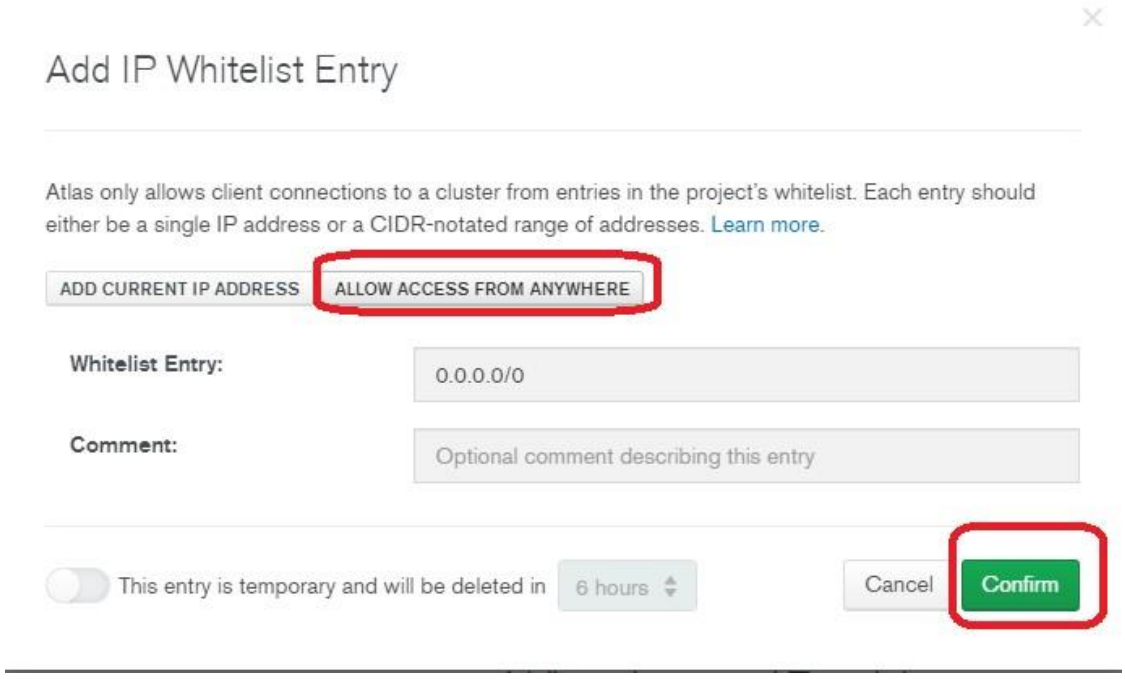

Figure 27 config IP

Next back to Clusters and click button Build a Cluster -> Create Cluster

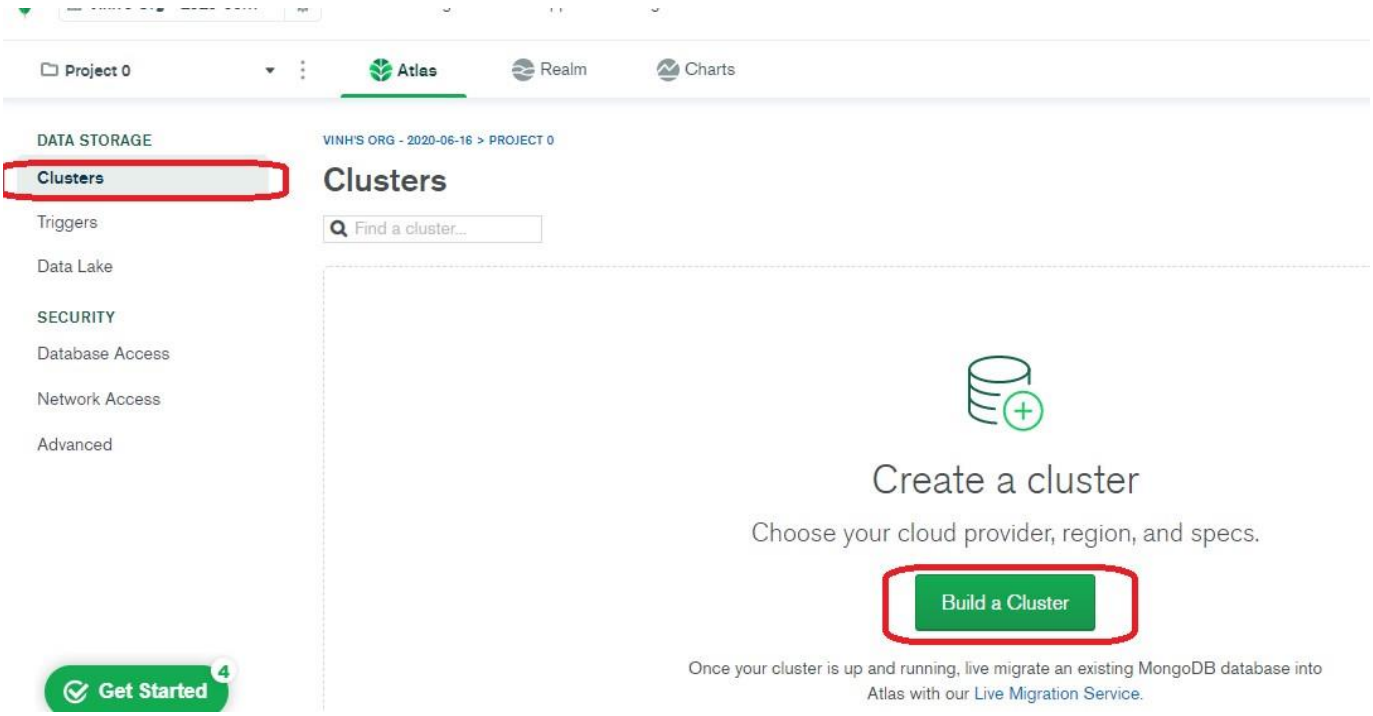

Figure 28 Build a Cluster

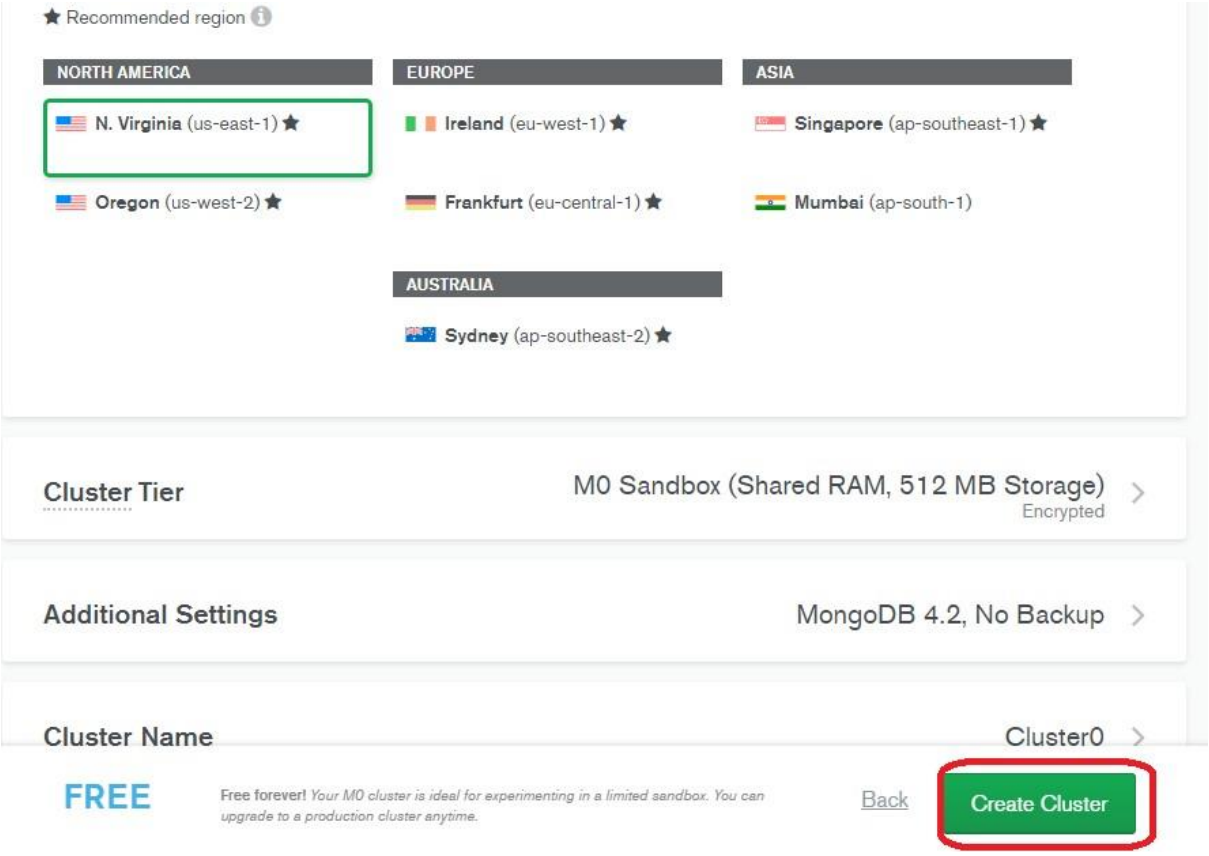

Figure 29 Create a cluster

Next click button Connect and then choose connect using mongodb compass

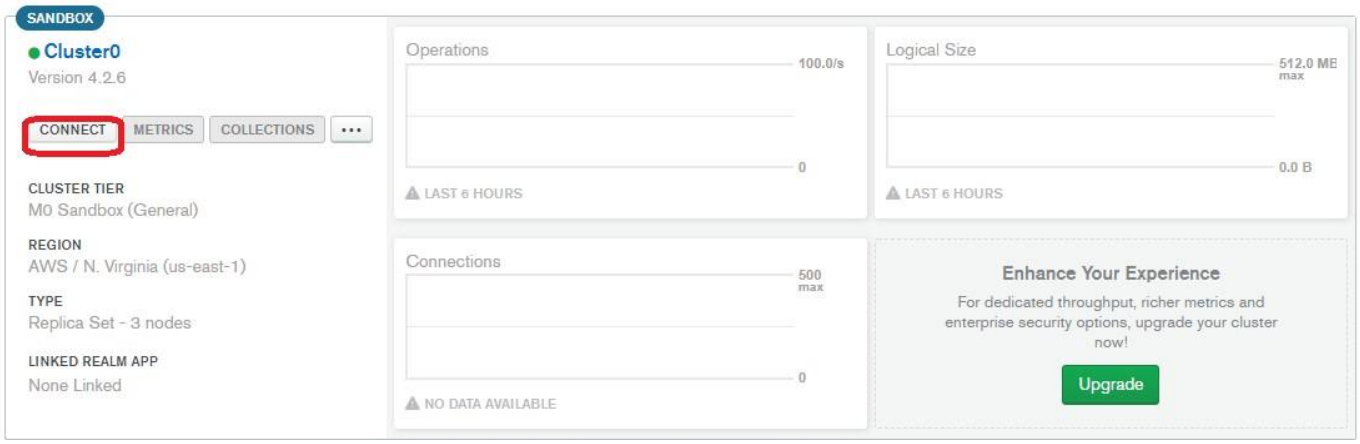

Figure 30 connect Cluster0

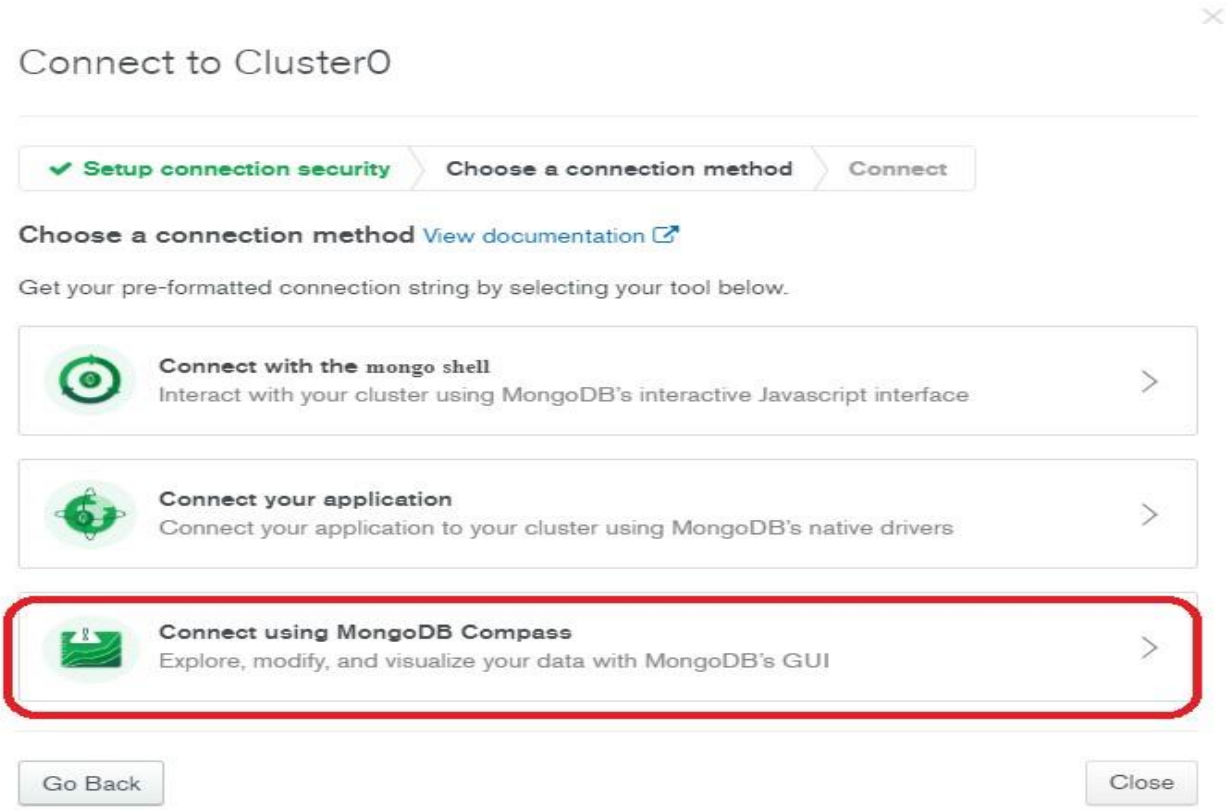

Figure 31 choose connect using MongoDB compass

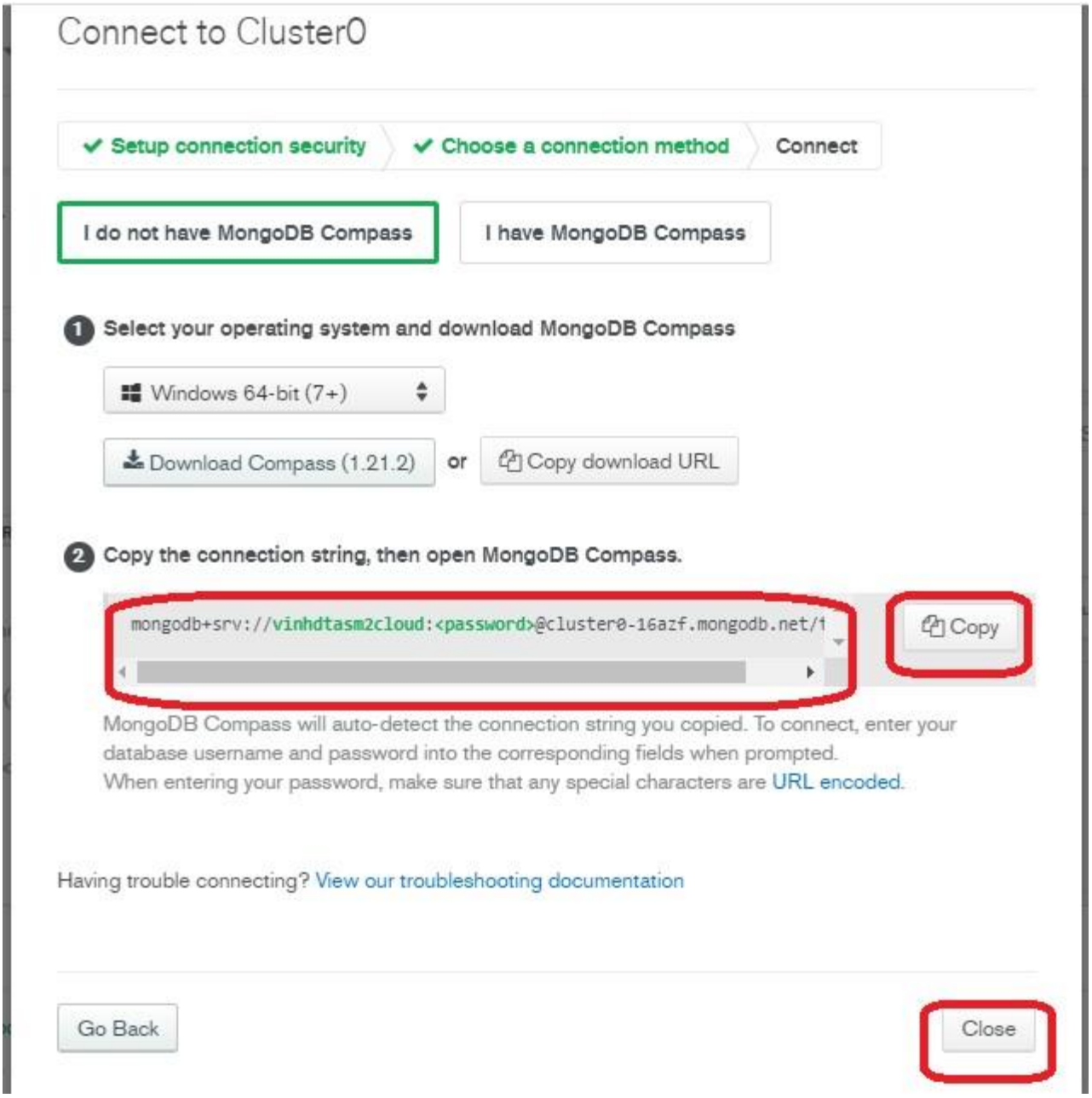

Figure 32 link to MongoDB

Final step is copy Link and paste to app MongoDB in desktop

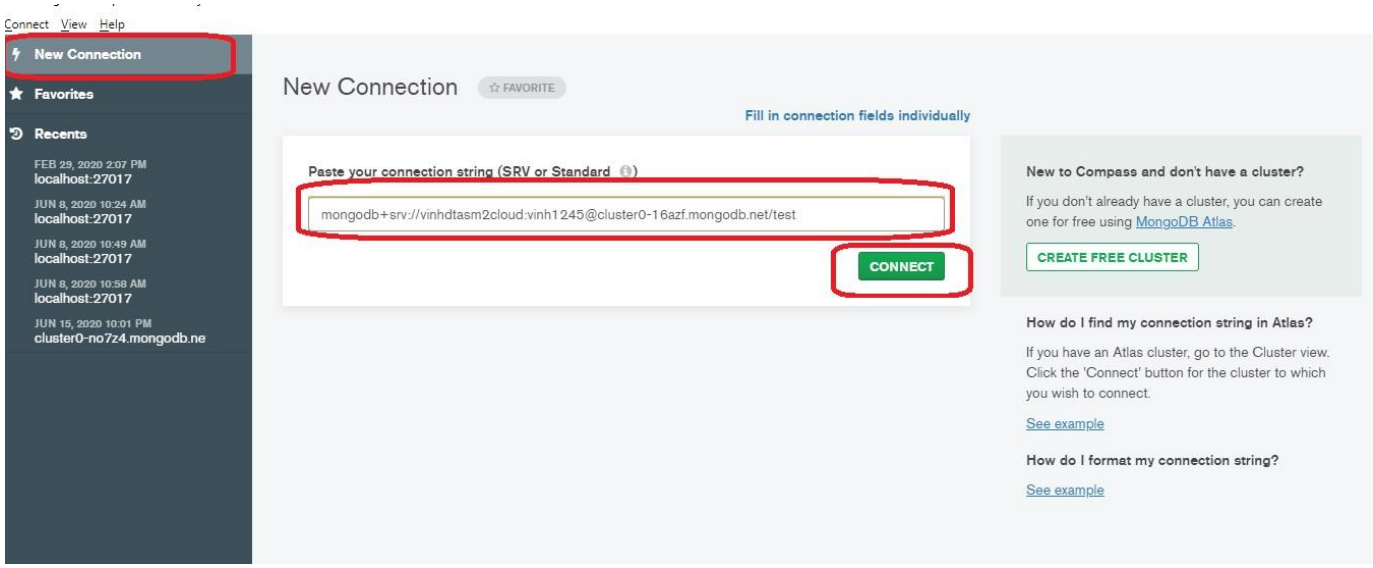

Figure 33 MongoDB in Desktop

First step copy Link in MongoDB Atlas and choose connect and wait

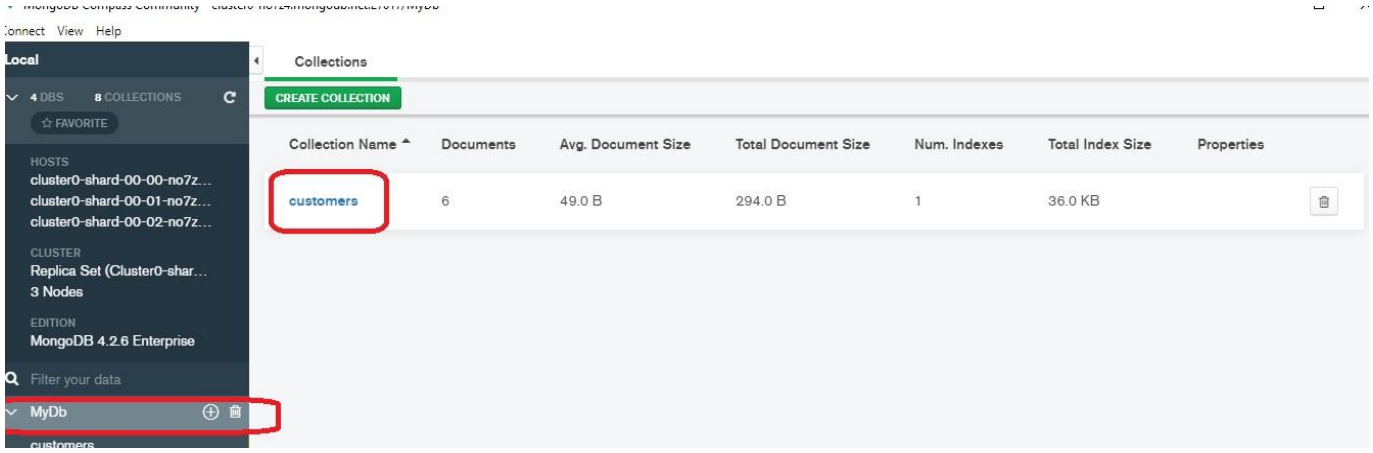

Figure 34 data after Create

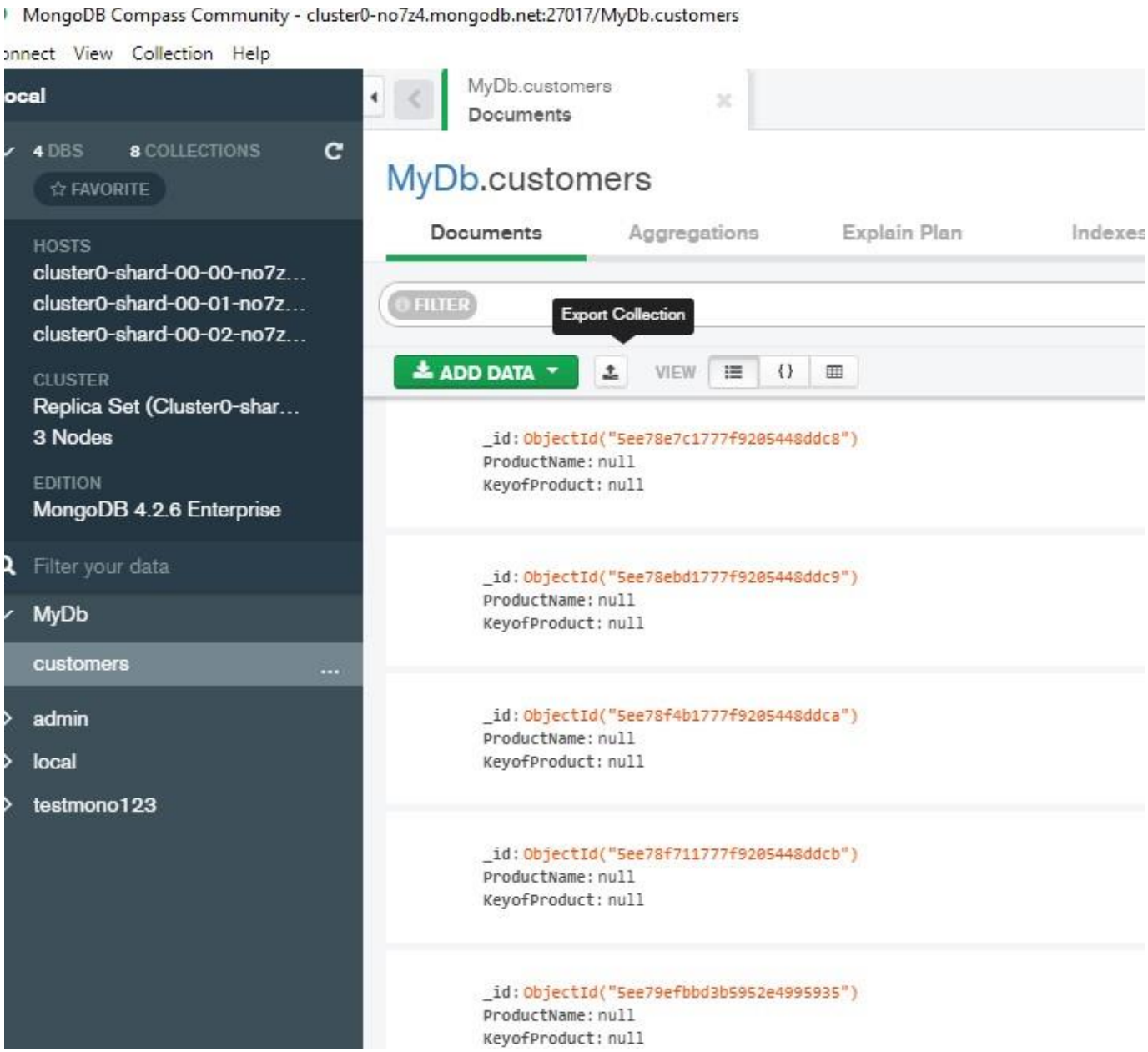

Figure 35 Data after insert

Source code connected to MongoDB and then insert and Delete product

```
var MongoClient = require('mongodb').MongoClient;
var url = 'mongodb+srv://vinhdtasm2cloud:vinh1245@cluster0-no7z4.mongodb.net/test/';

router.get('/',async (req,res)=>{
    let client= await MongoClient.connect(url);
    let dbo = client.db("MyDb");

    let results = await dbo.collection("customers").find({}).toArray();
    res.render('allCustomer',{customers:results});
})
```

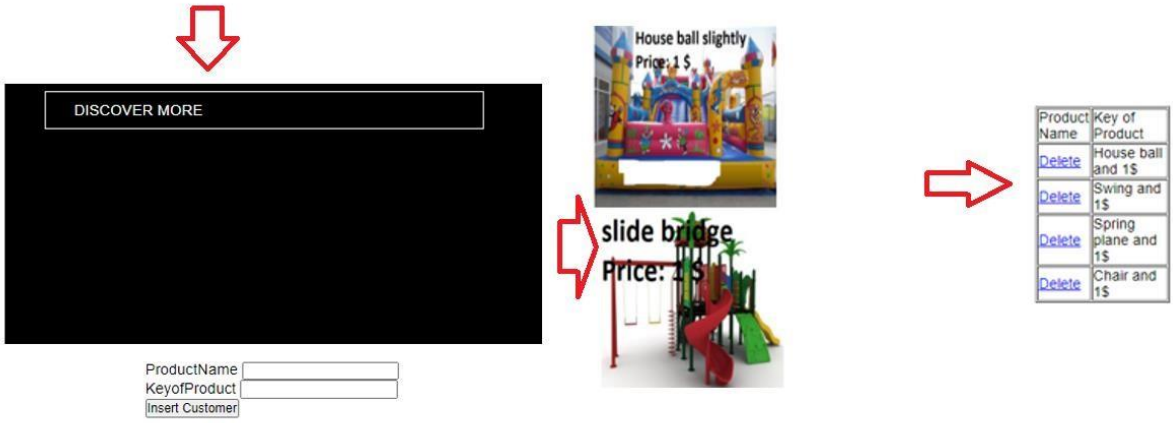

Figure 36 source code and step insert data

III. Common problems

Cloud use offers incentives for companies and enterprises even though they don't appreciate their infrastructure. Each organization or firm can choose to deploy a model that suits its needs. Cloud computing in general and deployment models in particular, however, also have problems worth considering

1. Public cloud

The most worrying issue with the Public model is the low level of data security. The public model is the one with the lowest data security of all four models. When an organization implements this model, it is the cloud service provider and not the organization that has the right to manage and store the data. Therefore, when they need to store and circulate information and documents internally, it's a huge obstacle for organizations and businesses. Besides, the control of the systems of these organizations is reduced by not having to buy physical hardware (instead of having to rent cloud services). (K. CHANDRASEKARAN, 2014)

- There's still a solution to this problem though. The solution is that consumers should hire the service from reliable cloud service providers, and there must be a transparent agreement between the customer and the cloud service provider. Customers need to know what kind of data, services, provider stores software and they need to commit to the provider what access rights and what

kind of information the provider will receive. On the supplier side, they have to commit to customers that confidentiality of information such as customer details, visitors, users, etc. When the two parties decide on the undertaking, all buyers and suppliers are obliged to respect the undertaking.

2. Private cloud

Private cloud provides high security and privacy to data, but there are several difficulties in setting up and maintaining this cloud. Users have to handle technology themselves, run, maintain and update the cloud infrastructure. Hence the expense of installing and maintaining a private cloud is much more costly than the expense of using a public cloud. In fact, only customers of the business or organization are allowed to use the private cloud services and infrastructure, and those who wish to connect must be approved.

- The company or organization may use the Data as a Service (DaaS) model to address the problem that business or organization partners who implement the private cloud must have an administrator or manager approval each time they need access to the network. This is a model of information delivery and distribution in which data files (including text, images, audio, and video) are delivered over the network to consumers, typically the Internet. This allows users to easily access applications and services that are available at anytime, anywhere, and on their own request.

3. Community cloud

Community clouds can be associated with many companies and organizations so community cloud setup, running, and operation have similarities like running a hospital or a school. Hence there will inevitably arise problems and risks. In addition, the community cloud meets privacy and security, and it enables rules to be set to comply with business-to-business cloud management policies, so building and deploying community cloud is expensive.

- In order to efficiently handle community cloud, corporations and organizations need to assign a cloud management individual (group), are the heads of organizations and enterprises, they are responsible for speeding up, collaborating with branch managers to get involved in community cloud administration. Therefore, they need to have a clear strategy to mitigate and deal with the issues that occur. Additionally, community-based companies and organizations should jointly develop rules and policies for cloud management and compliance implementation.

4. Hybrid cloud

Hybrid clouds are often a combination of two models: public cloud and private clouds so these models have both advantages and disadvantages. Companies often create hybrid clouds, and management responsibilities will be shared between the company and the public cloud provider. In fact, adopting a hybrid model is difficult as all models need to be worked on by organizations and businesses on the same project to find ways to improve the program. Hence the technical specifications and the implementation and operating costs are high. (Toby Velte, Anthony Velte, Robert C. Elsenpeter, 2009)

- You may select vendors that are cheap and professional with this model to reduce the small number of hybrid cloud companies and organizations. Joyent is a supplier that meets both requirements. Joyent has a lot of experience with the hybrid cloud model and is mindful of its drawbacks so many changes have been studied and made to best satisfy customer requirements. Joyent has become a common option for service providers needing low-cost large cloud data centers.

IV. Security issues and solution in cloud computing environment

Cloud computing has five main areas at risk of being compromised, and must therefore be kept confidential. They are below 5 areas.

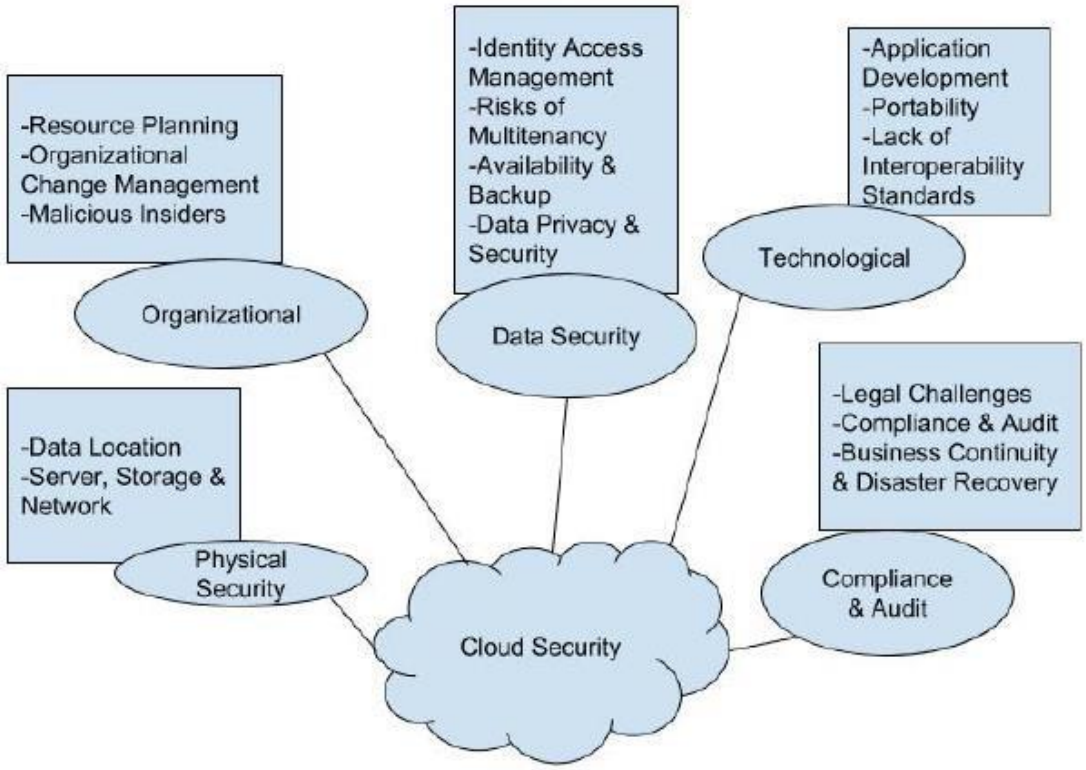

Figure 37 Cloud provider risk categories

1. Organizational Security Risks

   Organizational risk is considered a risk that may affect an organization or business structure. It's called being an entity. For example, if a cloud service provider goes bankrupt or is acquired by another company (entity), the Service Level Agreements (SLA) that they have previously issued may be changed so that cloud service customers may need to switch to a more appropriate cloud service provider. This change may lead to additional problems and costs. In addition, people in the organization can harm the use of data provided by users of their cloud services to malicious ends (Dahbur, K., Mohammad, 2013)

   - These companies may put strict legal binding clauses in the contract when recruiting workers to reduce the possibility of malicious workers inside the cloud service provider. In addition, they need to develop a strong notification process for security breaches.

2. Physical Security Risks

   Since even firewalls and encryption cannot completely protect data from theft, the cloud datacenter 's physical location should be applied with security measures to prevent unauthorized on-site access to customer data from the cloud services. Providers are in charge of infrastructure and are responsible for storing and processing data in specific jurisdictions so they are responsible for implementing appropriate infrastructure controls such as security of physical location, training of employees, building network firewalls. Additionally, they must comply with certain jurisdictions' regulations rules.

   - The physical security measures can prevent the threat of intruders having unauthorized physical access to devices in the cloud infrastructure. Such measures could be keycard access, biometric scans, so the possibility of reaching sensitive locations in the data center could be limited.

3. Technological Security Risks

   These are risks related to cloud service providers providing hardware, software, and services. For example, the multi-tenancy feature in the public cloud includes resource sharing isolation issues and risks linked to changing cloud service providers.

   - Cloud service providers may use various sources to verify a connection to mitigate the impact of this issue, and check if there are any sources associated with known malignant parties. In addition, they can also use Advanced Cloud Security (ACPS) to ensure guest virtual machines and distributed intermediaries are secure. They can track the behavior of cloud components by logging and periodically checking executable system files.

4. Compliance and Audit Risks

   These are risks linked to a lack of information on the authority, contractual provisions, changes in jurisdiction and legal disputes. For example, the information will be kept confidential, depending on the commitments between cloud service providers and customers. However, cloud service providers may be legally permitted to provide sensitive information or to transmit sensitive information when required by the government.

- In concerns relating to legal concerns, both cloud service providers and their customers need to consider the legal and ensure that arrangements made meet legal obligations and do not impact data privacy and protection.

5. Data Security Risks

Data security is a high-risk area that concentrates so much of the cloud security effort here. When it comes to data security, there are four main attributes to consider: privacy, data integrity, confidentiality and availability.

- Privacy ensures that cloud service customers ' personal information and identity is not disclosed to unauthorized users.
- Confidentiality is linked to data protection, as it guarantees that no unauthorized party is exposed to data belonging to clients of cloud services. Cloud service providers in the Public Cloud are responsible for customer data security. Since many tenants should have many customers accessing the same hardware that cloud service customers store their data on, however, the security becomes difficult.
- Confidentiality is linked to data protection, as it guarantees that no unauthorized party is exposed to data belonging to clients of cloud services. Cloud service providers in the Public Cloud are responsible for customer data security. Since many tenants should have many customers accessing the same hardware that cloud service customers store their data on, however, the security becomes difficult.
- Data integrity refers to the confidence that data stored in the cloud was not altered in any way when accessed by unauthorized parties. Thus, cloud service providers must ensure that data in transit or data in storage are not accessed by third parties.
- Availability is this feature that guarantees clients have access to their data and are not denied false access or due to any entity's malicious attacks. That means they must always be assured access to the data.

- Data flow through a cloud goes through various stages and issues of data security will occur during those stages. (Rohit Bhadauria, 2012)

- Data-in-transit phase: This is the time when data is transmitted to the cloud network or to customer-used computing equipment. The data are at the greatest risk of being intercepted at this point.

- Phase of data-at - rest is when the data is processed in the cloud infrastructure. The biggest issue for consumers at this point is that they are losing control of their data and service providers are responsible for defending against attacks during this process.
- Phase of the data in use is when the data is converted into information. The problem can lie during this step in the data being corrupted while it is being processed.

Figure 38 Information security component

V. Some issues when developing the ATN web site

Applying a cloud infrastructure platform to build websites for ATN companies offers a lot of benefits but this also has some challenges that create development process difficulties. The first requisite is the internet. Because all need to connect to the Internet to access and work with Heroku, GitHub and MongoDB, developers can only work when they are able to connect to the Internet. The second problem is the loss of the Database connection. The website's database server is MongoDB's server, and it is managed by Mongo Atlas so the connection is sometimes interrupted in the process of database development, so MongoDB cannot execute query commands. To solve this, the developer had to adjust the internet that the machine was connected to another network because getting so many users accessing MongoDB on the same network IP range at a time would cause problems. The economy. The third issue is the delay of code deployment to GitHub and Heroku. Even the smallest one must commit

changes to the NodeJS file and push it to GitHub when there is any change in the code. Additionally, GitHub only allows each individual NodeJS file to be committed, meaning how many NodeJS files have code changes, they have to commit multiple times. The file changes in GitHub must then be deployed to Heroku. Although this process takes only about 15-20 seconds, as it takes a lot of time in the process of development, it leads developers to spend a lot of time on this. The time it takes for GitHub and Heroku to process is immutable so developers carefully check the code before uploading to GitHub and connecting the computer to the Internet to reduce this waste of time. High speed to constrain processing time. Additionally, the security threats of technology are also a source of concern. Since all of the technology, the base of this website relies on Heroku, the site will be down, or unavailable, etc. if something goes wrong with the Heroku cloud. However, this is rare since the technology of Heroku is stored and managed in the protected data centers of Amazon and uses an Amazon service called the AWS (Amazon Web Services). Responsible for on-going risk management and standard periodic reviews.

VI. Conclusion

Cloud computing application brings a lot of advantages and opportunities for organizations and businesses to develop but along with it are the risks of data security, technical, legal and organizational. These risks can be mitigated by applying a number of methods which are specific to each company. In addition, cloud service models also have problems with what organizations and businesses need to consider in implementing the appropriate model. In addition, this article also shows how to deploy the website of the ATN company based on the cloud computing platform and some binding issues in the implementation process to give a small example of deploying a cloud computing platform based on the web.

References

Dahbur, K., Mohammad, 2013. *jisajournal,An analysis of security issues for cloud computing.* [Online] Available at: https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5 [Accessed anon anon].

K. CHANDRASEKARAN, 2014. *Essentials of CLOUD.* s.l.:s.n.

Rohit Bhadauria, 2012. *(Cornell University)Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques.* [Online]
Available at: https://arxiv.org/abs/1204.0764 [Accessed
anon anon 2012].

Toby Velte, Anthony Velte, Robert C. Elsenpeter, 2009. *Cloud Computing: A Practical Approach.* s.l.:s.n.