

Tuần 8

EC2 và S3

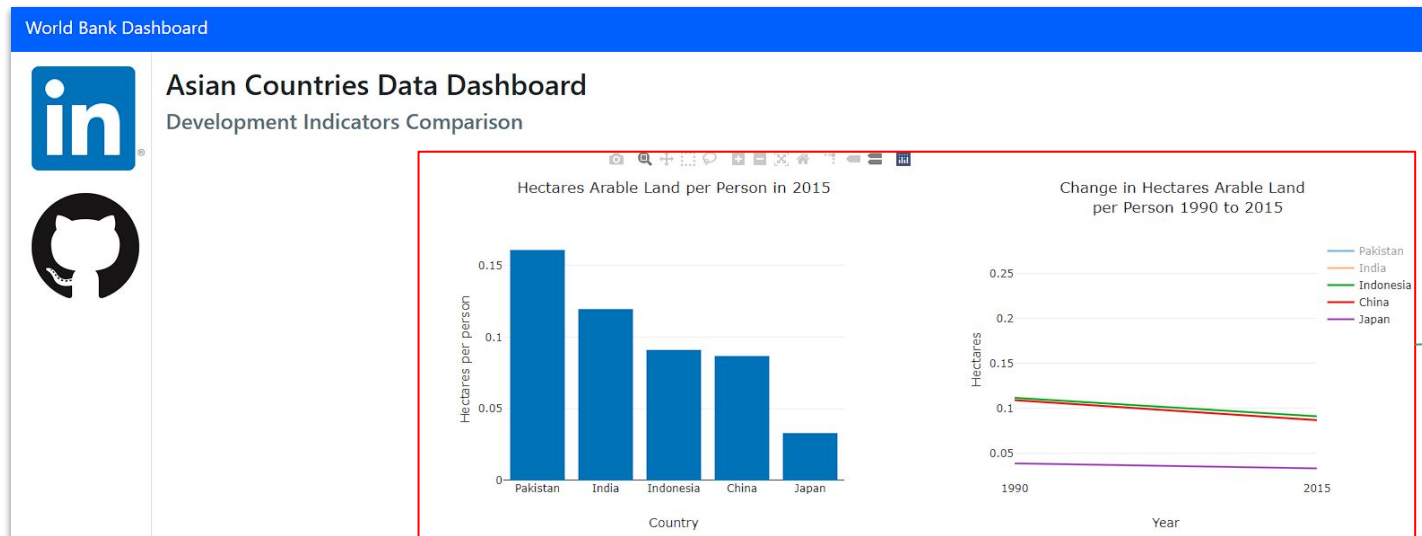
TS. Phạm Tuấn

ptuan@ute.udn.vn

Giới thiệu

Chúng ta sẽ xây dựng trang web như sau với 2 thành phần:

- Trang web ở EC2
- Dữ liệu được lấy từ S3



Dữ liệu biểu đồ
được lưu ở S3

Tạo EC2 Instance và S3

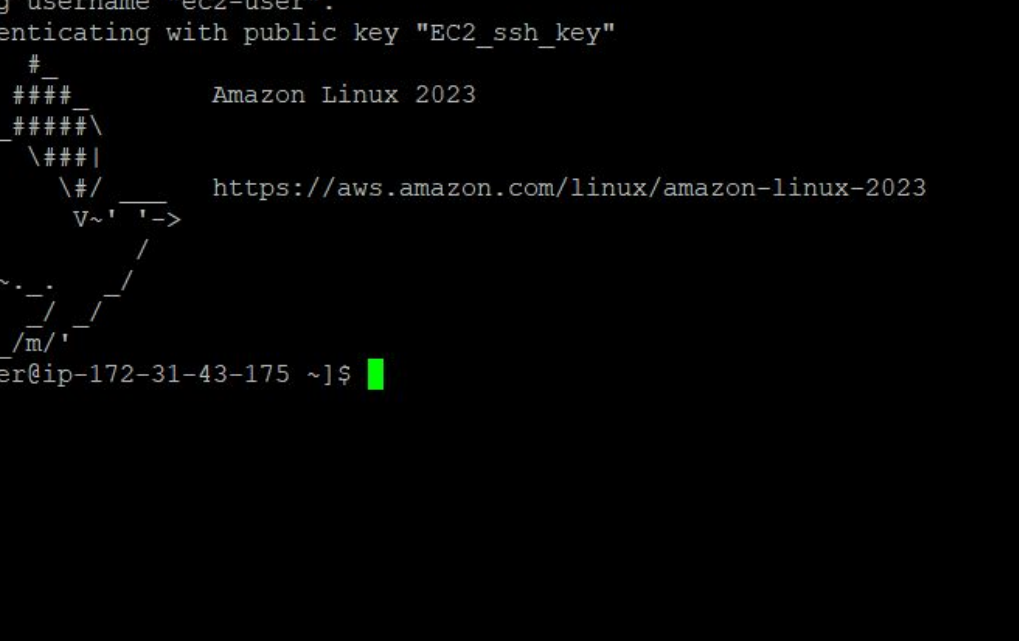
Tạo một EC2 Instance mới một số configuration như sau:

- **Name:** web-dashboard
- **OS:** Amazon Linux 2023 AMI
- **Instance type:** t2.micro
- **Key pair:** ec2_ssh_key
- **Allow SSH:** My IP
- **Allow Custom TCP, Port: 8080, Source: 0.0.0.0**

Tạo một S3 Bucket mới một số configuration như sau:

- **Name:** web-dashboard-**yourname**

SSH đến EC2 Instance



```
ec2-user@ip-172-31-43-175:~  
Using username "ec2-user".  
Authenticating with public key "EC2_ssh_key"  
#  
~\#####_ Amazon Linux 2023  
~~\#####\  
~~\#####|  
~~\#/ https://aws.amazon.com/linux/amazon-linux-2023  
~~V~'-'>  
~~~  
~~-.-  
~~/m/'-  
[ec2-user@ip-172-31-43-175 ~]$
```

Download source code

Chúng ta download web dashboard bằng command sau:

```
wget --no-check-certificate  
'https://docs.google.com/uc?export=download&id=1NBKMvLj6Y7Bphgj8JnqcE5LdPsGUyKzr' -O  
web-dashboard.zip
```

Sau đó chúng ta unzip bằng câu lệnh sau:

```
unzip web-dashboard
```

```
[ec2-user@ip-172-31-43-175 ~]$ ls  
Python-Flask-Data-Dashboard  web-dashboard.zip
```

Install python và các thư viện cần thiết

sudo yum install python

sudo yum install python-pip

Chúng ta cd Python-Flask-Data-Dashboard để truy cập source code

```
[ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ ls
README.md  data          worldbank.py  wrangling_scripts
config     requirements.txt worldbankapp
```

Chúng ta gõ câu lệnh sau để install các library cần thiết để chạy source code

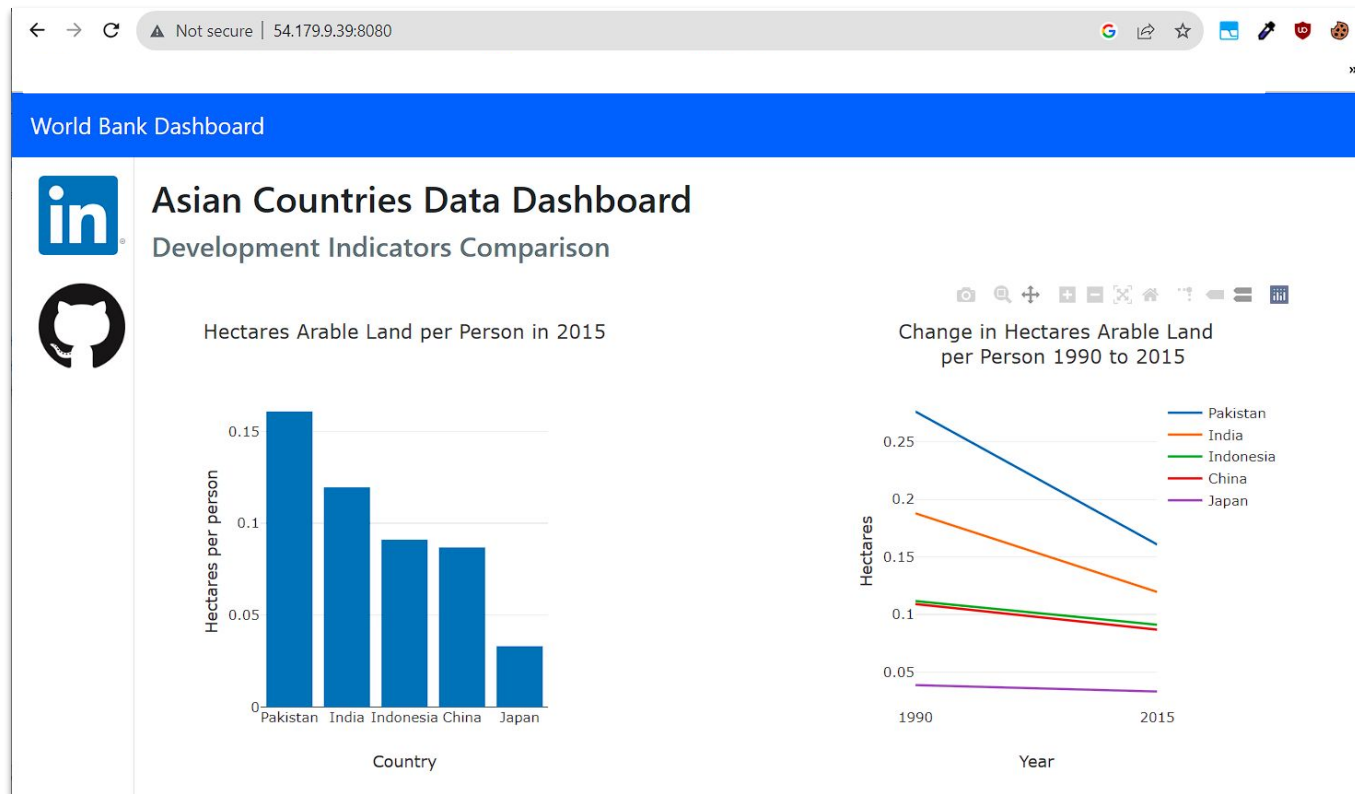
pip install -r requirements.txt

Sau đó chúng ta chạy lệnh sau để khởi chạy dashboard:

python worldbank.py

Giao diện của web-dashboard

Sau khi khởi chạy thành công, chúng ta nhấn Ctrl+c để tắt web-dashboard đang chạy



Attach IAM role vào EC2

EC2 > Instances > i-0a029372cc3c6650f

Instance summary for i-0a029372cc3c6650f (web-dashboard) [Info](#)

Updated less than a minute ago

Instance ID i-0a029372cc3c6650f (web-dashboard)	Public IPv4 address 54.179.9.39 open address	Private IPv4 addresses 172.31.43.175	<div>Instance state ▼</div> <div>Actions ▲</div> <div><div>Connect</div><div>Manage instance state</div><div>Instance settings ▶</div><div>Networking ▶</div><div>Security ▶</div><div>Image and templates ▶</div><div>Monitor and troubleshoot ▶</div></div>
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-179-	
Hostname type IP name: ip-172-31-43-175.ap-southeast-1.compute.internal	Private DNS name (IPv4 only) ip-172-31-43-175.ap-southeast-1.compute.internal	Change security groups Get Windows password Modify IAM role	
Answer private resource DNS name IPv4 (A) -	Instance type t2.micro	Elastic IP addresses -	
Auto-assigned IP address 54.179.9.39 [Public IP]	VPC ID vpc-0f79fe5495702a440	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-03c8985265a68fde2		
IMDSv2 Required			

Tạo IAM role


Chúng ta tạo một IAM role
và sau đó attach vào EC2

[EC2](#) > [Instances](#) > [i-0a029372cc3c6650f](#) > **Modify IAM role**

Modify IAM role [Info](#)

Attach an IAM role to your instance.


Instance ID


 [i-0a029372cc3c6650f](#) (web-dashboard)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role ▼

 [Create new IAM role !\[\]\(73db7566b2c84a73d9014101bf098e56_img.jpg\)](#)

 If you choose **No IAM Role**, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?

Cancel

Update IAM role

Tạo IAM role

[IAM](#) > Roles

Roles (3) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

[Refresh](#) [Delete](#) [Create role](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing(S	13 days ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support(Service-Linker	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor(Service	-

Roles Anywhere [Info](#)

Authenticate your non AWS workloads and securely provide access to AWS services.

[Manage](#)



Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.



X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.



Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Tạo IAM role

Select trusted entity [Info](#)

Trusted entity type

☒ **AWS service**

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

☐ **EC2 - Scheduled Instances**

Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel

Next

Cấp quyền truy cập S3 cho IAM role

Add permissions [info](#)

Permissions policies (1/885) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type All types 9 matches

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings for...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the ...
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permissi...
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on Out...
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S3 o...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets vi...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Backup	AWS managed	Policy containing permissions necessary f...
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Restore	AWS managed	Policy containing permissions necessary f...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	Policy used by QuickSight team to access ...

► Set permissions boundary - optional

Cancel Previous **Next**

Thực tế, người ta sẽ tạo một policy để gán quyền truy cập vào một S3 cụ thể thay vì FullAccess

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

web-dashboard-IAM

Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters.

Description

Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Step 1: Select trusted entities

Edit


Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    }  
15  ]  
16 }
```

Step 2: Add permissions

Edit

Permissions policy summary

Policy name 	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Update IAM role

[EC2](#) > [Instances](#) > [i-0a029372cc3c6650f](#) > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

 [i-0a029372cc3c6650f](#) (web-dashboard)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

web-dashboard-IAM



[Create new IAM role](#) 

Cancel

Update IAM role

Kiểm tra IAM role

Kiểm tra EC2 instance đã truy cập được vào S3 chưa

```
[ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ aws s3 ls
2023-10-31 11:33:40 test-s3-tuanp
2023-10-31 11:06:59 web-dashboard-tuanp
[ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$
```

Mount bucket vào một folder của EC2

Chúng ta chạy các lệnh sau để mount bucket vào một folder của EC2 instance

```
wget https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
```

```
sudo yum install ./mount-s3.rpm
```

```
mkdir s3-bucket-data
```

```
ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ mkdir s3-bucket-data
ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ mount-s3 web-dashboard-tuanp s3-bucket-data
bucket web-dashboard-tuanp is mounted at s3-bucket-data
ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$
```


Upload dữ liệu lên S3

[Amazon S3](#) > [Buckets](#) > web-dashboard-tuanp

web-dashboard-tuanp [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	arableland.csv	csv	October 31, 2023, 19:37:10 (UTC+07:00)	279.3 KB	Standard

Sau khi chúng ta upload file lên S3, chúng ta kiểm tra đã thấy file từ EC2 chưa

```
[ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ cd s3-bucket-data/  
[ec2-user@ip-172-31-43-175 s3-bucket-data]$ ls  
arableland.csv
```

Xóa dữ liệu trên EC2

Chúng ta xóa dữ liệu của dashboard bằng câu lệnh sau:

```
rm -r data/
```

Chúng ta chạy lệnh sau để khởi chạy dashboard, và sẽ thấy lỗi.

```
python worldbank.py
```



Config lại path

Chúng ta chỉnh sửa lại đường dẫn để dashboard nhận dữ liệu từ S3.

```
[ec2-user@ip-172-31-43-175 Python-Flask-Data-Dashboard]$ nano config/constant.py
```

```
GNU nano 5.8
```

```
CSV_PATH = 's3-bucket-data/arableland.csv'
```

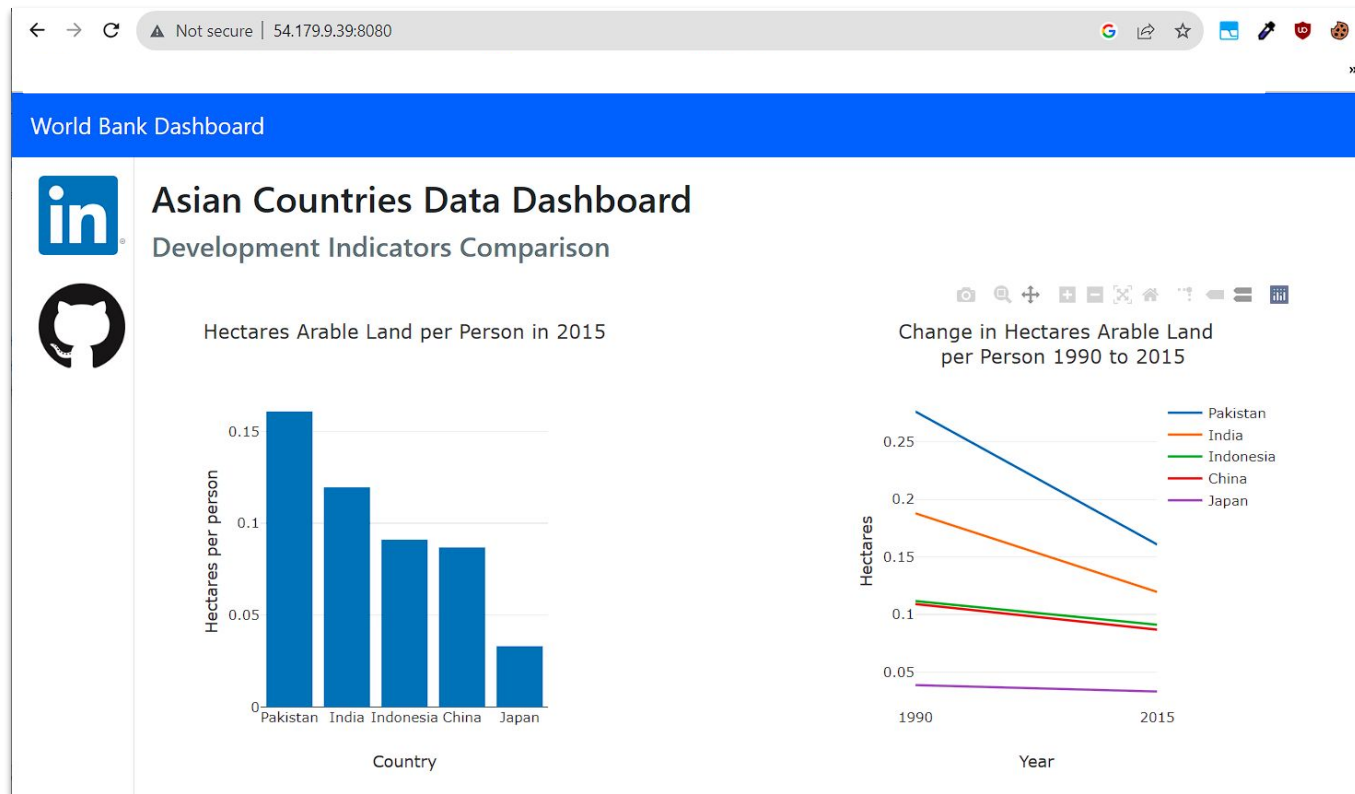
Ctrl+X -> Y -> Enter để save file

Giao diện của web-dashboard

Chúng ta chạy lệnh sau:

```
python worldbank.py
```

Và kiểm tra web dashboard
đã load thành công file từ S3



Any questions ?

