Setup Documents of Server

TODO: Write a project description

SSH Security

a. SSH keys login only:

- https://help.ubuntu.com/community/SSH/OpenSSH/Keys#Key-Based_SSH_Logins
- Generate RSA Keys in client

```
mkdir ~/.ssh
chmod 700 ~/.ssh
ssh-keygen -t rsa
```

- Configure key pair as below:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/b/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/b/.ssh/id_rsa.
Your public key has been saved in /home/b/.ssh/id_rsa.pub.
```

- update authorized_keys

```
cp authorized_keys authorized_keys_Backup
cat id_rsa.pub >> authorized_keys
```

- testing:

```
ssh root@localhost
```

- You should be prompted for the passphrase for your key:

```
Enter passphrase for key '/home/<user>/.ssh/id_rsa':
```

- **Download you id_rsa from filezilla !!!**

b. Disable password login:

```
/etc/ssh/sshd_config  -> #PasswordAuthentication no
sudo service ssh restart
```

c. Enable FTP on FileZilla

```
upload id_rsa to FileZilla to get ppk
```

d. Create Iptable rules

- create iptables files (reference on iptables.example.txt)

```
iptables-apply iptables
```

e. Update rc.local

- reference on (rc.local.example.txt)

```
vi /etc/rc.local
```

f. Prepare MySQL/ Python-Mysql

```
sudo apt-get install mysql-server-5.6
apt-get install python-dev libmysqlclient-dev
wget https://bootstrap.pypa.io/get-pip.py
pip install MySQL-python
crontab -e
add /usr/bin/python2 /var/www/data_portal/cron/expiry_sweeper.py
```