# SMPC Deployment Handbook

### Overview of the cloud setup

1. **Remote split version**

* Two cloud VMs - smpc-server0 and smpc-server1

1. **CNN split version**

* Two cloud VMs - smpc-server0 and smpc-server1

1. **Helper node version**

* Three Cloud VMs - smpc-server0, smpc-server1, smpc-server2

### Cloud Servers Info

|  | **Azure Cloud VM 0 (smpc-server0)** | **AWS Cloud VM 1 (smpc-server1)** | **AWS Cloud VM2 (smpc-server2)** |
| --- | --- | --- | --- |
| **Public IP** | 20.197.27.117 | **13.200.145.195** | 15.206.80.191 |
| **Private IP** | 10.139.0.4 | 10.2.1.25 | 10.2.1.171 |
| **ssh** | ssh ubuntu@20.197.27.117 | ssh ubuntu@13.200.145.195 | ssh ubuntu@15.206.80.191 |
| **instance** | Azure - b1s  1vcpu, 1 GiB, 30 GiB SSD | t2.micro  (1vcpu, 1GiB, 30 GiB SSD) | t2.nano  1vcpu, 0.5GiB, 30 GiB SSD |
| **Network** |  | subnet: iudx-test-1  VPC: iudx-test | subnet: iudx-test-1  VPC: iudx-test |

### Config File Setup (Paste at)

The config files utilised/read are as follows

##### SMPC Config:

Required in all setups

* Remote Split Setup smpc-split-config.json
* CNN Split Setup smpc-cnn-config.json
* Helper Node Setup smpc-helpernode-config.json

##### Model Config:

Requires Only for Model Provider in all setups

* Remote Split Setup model\_split\_config.json
* CNN Split Setup model\_cnn\_config.json
* Helper Node Setup model\_helpernode\_config.json

##### Image Config

Required Only for Image Provider in Server Model only

* All setups image\_config.json

### Available Models (Copy from)

##### 2 Layer NN (The Split Model)

Model Config: config\_files/example-model\_split\_config.json

Recommended Split Info: config\_files/example-smpc-split-config.json

##### 5 Layer NN (The helpernode Model)

Model Config: config\_files/example-model\_helpernode\_config.json

Recommended Split Info: config\_files/example-smpc-split-config.json

##### 3 Layer CNN

Model Config: config\_files/ex-1l\_mnist-model\_cnn\_config.json

Recommended Split Info: {"layer\_id":2, "rows":100, "splits":2}

##### 4 Layer CNN

Model Config: config\_files/ex-2l\_mnist-model\_cnn\_config.json

Recommended Split Info: {}

##### CIFAR CNN

Model Config: config\_files/example-model\_cnn\_config.json

Recommended Split Info: config\_files/example-smpc- t-config.json

### Non Server Model wo Docker:

#### Split:

***bash scripts/Non-ServerModel\_Architecture/Split/remote\_server0\_split.sh***

***bash scripts/Non-ServerModel\_Architecture/Split/remote\_server1\_split.sh***

#### Helpernode:

***bash scripts/Non-ServerModel\_Architecture/HelperNode/helpernode\_server0.sh***

***bash scripts/Non-ServerModel\_Architecture/HelperNode/helpernode\_server1.sh***

#### CNN:

***bash scripts/Non-ServerModel\_Architecture/Split/CNN/remote\_server0\_split\_CNN.sh***

***bash scripts/Non-ServerModel\_Architecture/Split/CNN/remote\_server1\_split\_CNN.sh***

### Server Model:

#### CNN:

Server 0:

***cd scripts/ServerModel\_Architecture/Split/CNN***

***docker compose -f docker-compose.cnn\_split\_servermodel.yaml -f ../../../../docker-compose.remote-registry.yaml up -d smpc-server0***

Server 1:

***cd scripts/ServerModel\_Architecture/Split/CNN***

***docker compose -f docker-compose.cnn\_split\_servermodel.yaml -f ../../../../docker-compose.remote-registry.yaml up -d smpc-server1***

Model Provider:

***bash scripts/ServerModel\_Architecture/Split/CNN/ModelProvider\_CNN.sh***

Image Provider:

Terminal 1:

***autossh -M 23323 -N -q -o "ExitOnForwardFailure yes" -o "ServerAliveInterval 10" -o "ServerAliveCountMax 3" -R 4007:localhost:4007 sshtunuser@analytics.iudx.org.in -i ~/.ssh/iudx\_cloud***

Terminal 2:

***autossh -M 23325 -N -q -o "ExitOnForwardFailure yes" -o "ServerAliveInterval 10" -o "ServerAliveCountMax 3" -R 4008:localhost:4008 sshtunuser@analytics.iudx.org.in -i ~/.ssh/iudx\_cloud***

Terminal 3:

***bash scripts/ServerModel\_Architecture/Split/CNN/ImageProvider.sh***

nano ../../../../config\_files/smpc-cnn-config.json

docker exec -it <container\_id> bash