

SOSCON

Let's build IoT with privacy in mind

Samsung Research UK | Open Source Group | Ziran Sun & Philippe Covel
October 2019



Content

Why Privacy in IoT?

Build a Smart Home with Web of Things

Modelling Your Smart Home with Digital Twins

Data Protection for Large-scale IoT with FL

01

02

03

04



SOSCON2019

SAMSUNG OPEN SOURCE CONFERENCE 2019

1. Why Privacy in IoT?



Privacy in IoT

- Risk of loss of privacy in IoT is **HIGH!!!!**
- GDPR
 - ✓ Protects personal data in law
 - ✓ Advocates “Data protection by design” or “privacy by design”
- Open web platform promises enhanced privacy

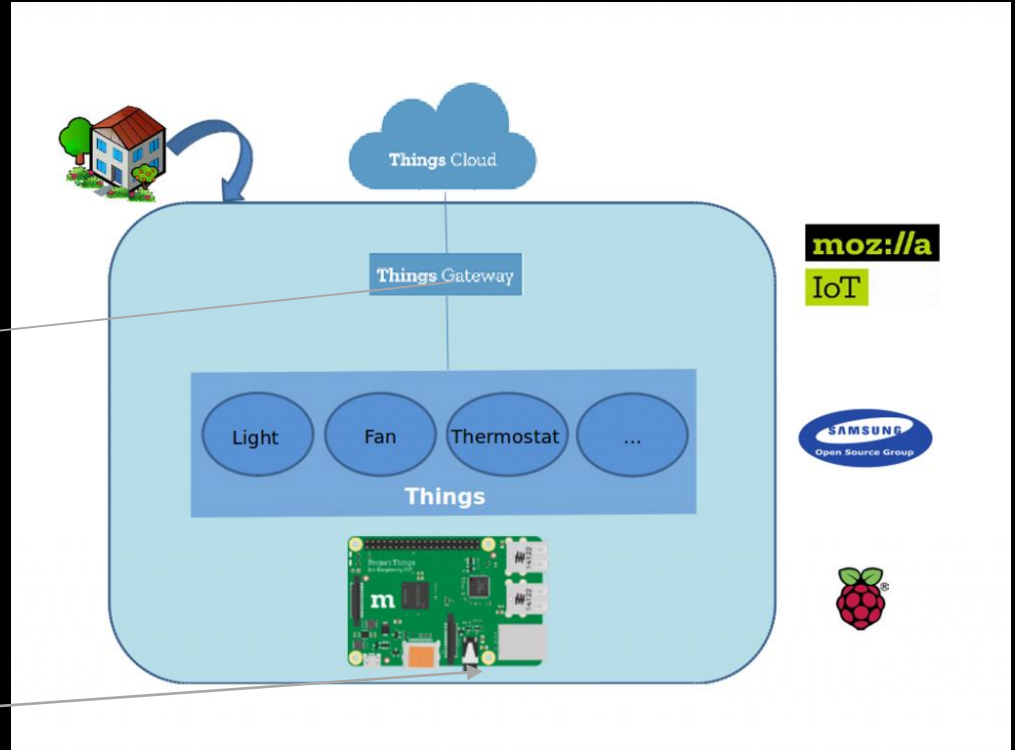


2. Build a Smart Home with Web of Things

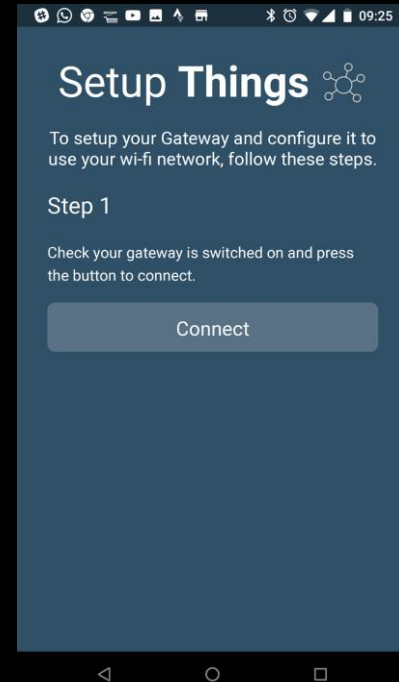


- Addresses interoperability challenge in IoT
- An application layer solution for IoT
- Specification work led by W3C

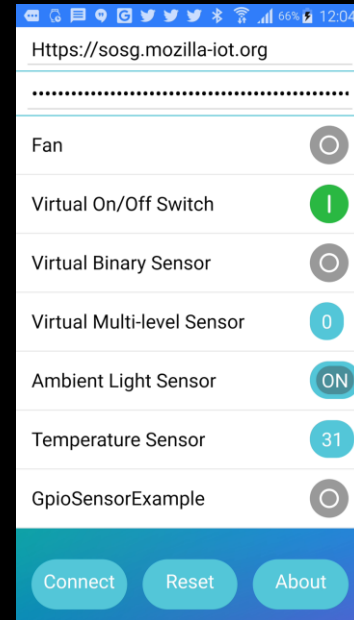


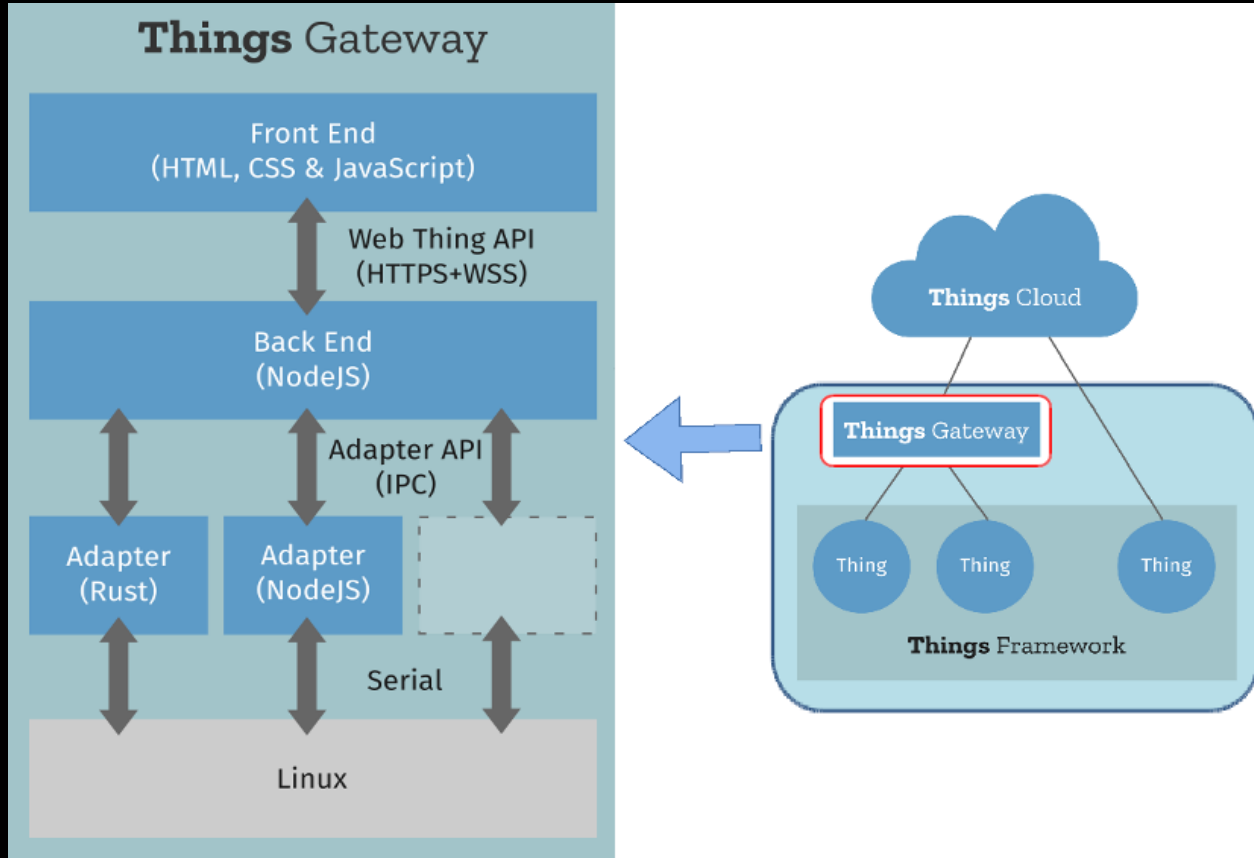


- PWA in the control device uses BLE to scan and pair with the new device
- PWA device authenticates with the new device
- PWA device pass WiFi details to the authenticated new device via BLE channel
- New device uses obtained WiFi information to connect to the home WiFi



- Websites that deliver native app-like user experiences
 - “Add to Home Screen” prompts
 - Offline functionality
 - Fast loading from cache
 - (Optionally) web push notifications
- Only served over HTTPS





- HTTPS via mozilla-iot.org tunnelling service
- Allow setting up a secure subdomains with LetsEncrypt TLS certificates
- TCP tunnel uses PageKite from Mozilla cloud server to Gateway
- OAuth to authorize third party apps & services
- JSON Web Tokens (JWT) used for authentication



3. Modelling Your Smart Home with Digital Twins



- Digital replica of living or non living entity
 - Real time (or deferred) connectivity
- “Devices as service” concept:
 - Pre/Co/Re/Design (products and services)
 - Impact analysis, simulation, playback
 - Improve decision making
- Domains:
 - Industry (4.0), (Smart) City to generic uses
- Digital Twins on The Web : **Web of Twins**



<https://libraries.io/npm/color-sensor-js>

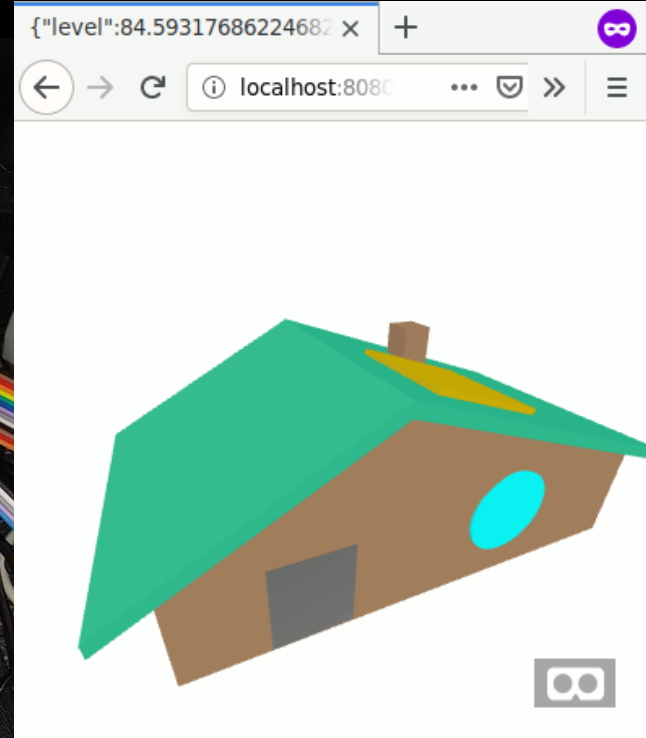


- From Low End Devices: MCU on IoT.js / JerryScript
 - REST API using *webthing-iotjs*
 - IO: GPIO, ADC, PWM, I2C: *generic-sensors-lite*
 - Handled by Mozilla IoT Gateway
- To Web Browser
 - Security handled with JSON Web Token (JWT)
 - 3D rendering using *A-Frame* framework (WebXR)
 - Real time animation using WebSockets (or HTTP)



Getting started with "Solar House"

SOSCON2019



Demo application (with simulator, GLTF model)

<https://npmjs.com/package/aframe-smart-home>

Bridge from WebThings to A-Frame

<https://npmjs.com/package/aframe-webthing>

Robotic Arm for MCU and XR

<https://www.npmjs.com/package/twins>

More on wiki page:

<https://github.com/rzr/webthing-iotjs/wiki/DigitalTwins>

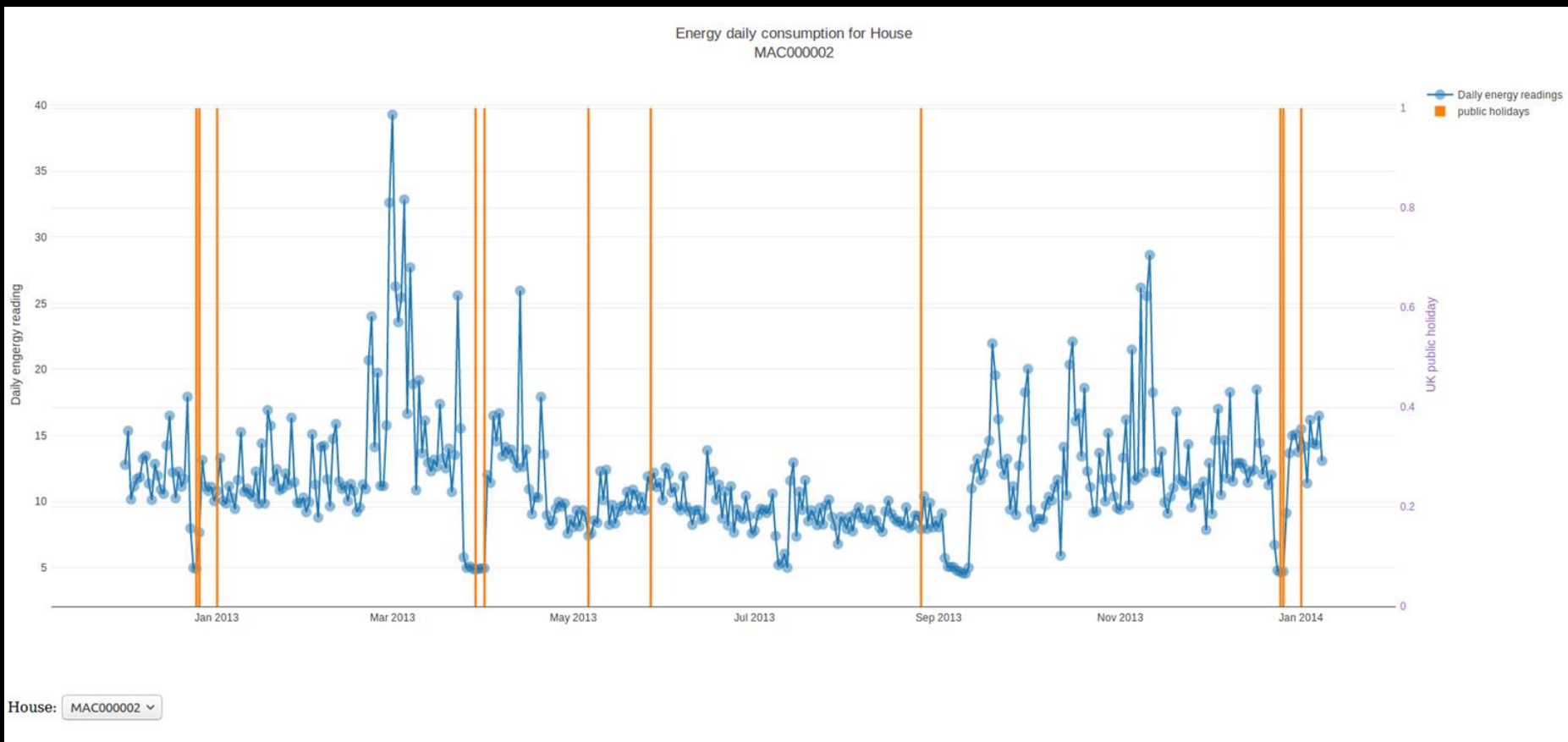


4. Data Protection for Large-scale IoT with FL



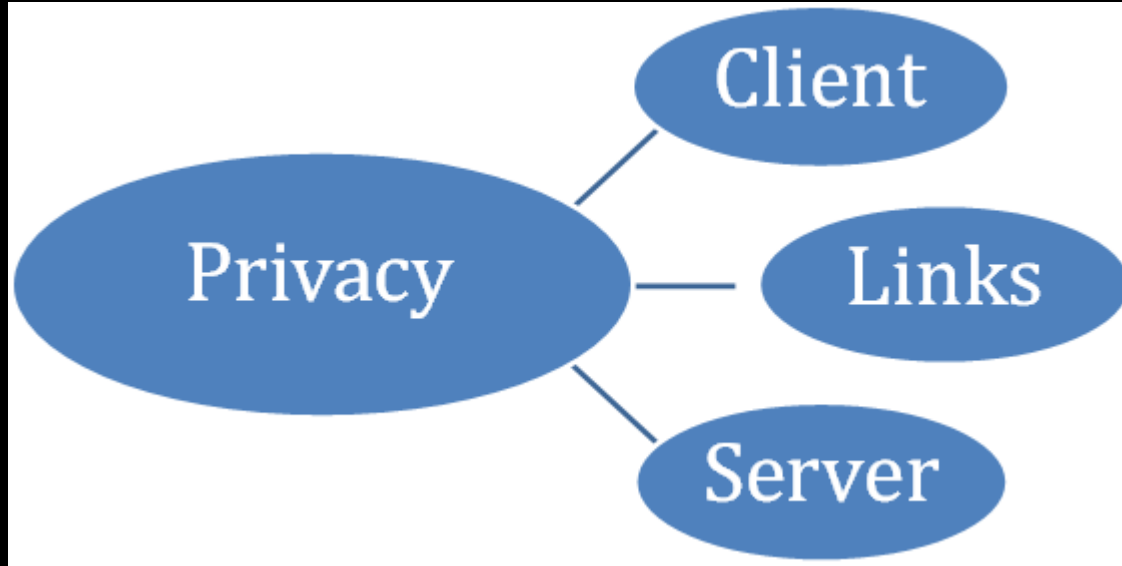
Playing with raw data?

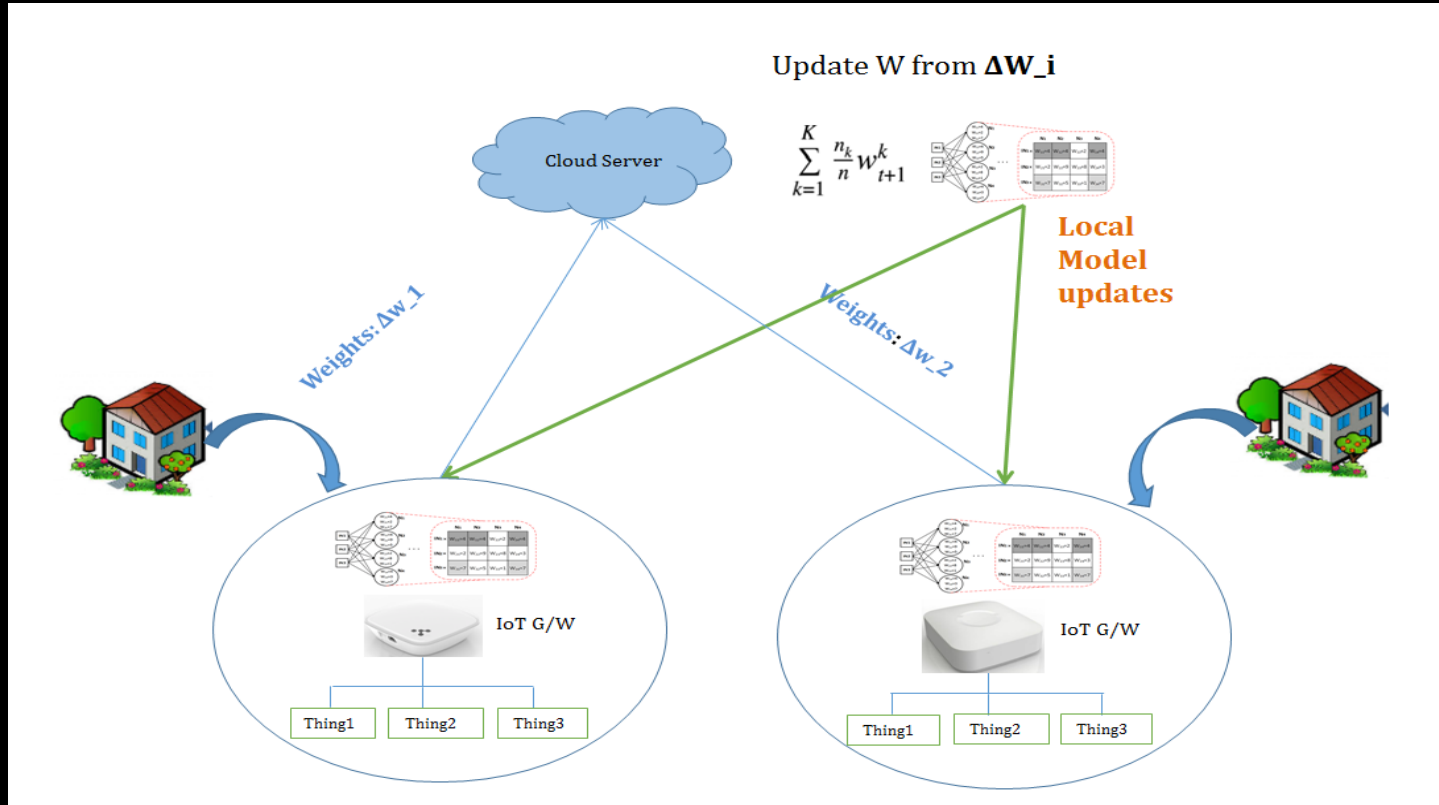
SOSCON2019



- Decentralized
- Privacy
- Possible Personalized for a user







FL_Demo_Video



```

File Edit View Search Terminal Help
WARNING:tensorflow:From /usr/local/lib/python3.7/site-packages/tensorflow/python
/framework/op_def_library.py:263: colocate_with (from tensorflow.python.framework
k.ops) is deprecated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
Loading global model weights...
2019-05-31 13:01:46.895994: I tensorflow/core/platform/cpu_feature_guard.cc:141]
Your CPU supports instructions that this TensorFlow binary was not compiled to
use: AVX2 FMA
2019-05-31 13:01:46.900122: I tensorflow/core/platform/profile_utils/cpu_utils.c
c:94] CPU Frequency: 3597695000 Hz
2019-05-31 13:01:46.900712: I tensorflow/compiler/xla/service/service.cc:150] XL
A service 0x7f90b41ed6a0 executing computations on platform Host. Devices:
2019-05-31 13:01:46.900755: I tensorflow/compiler/xla/service/service.cc:158]
StreamExecutor device (0): <undefined>, <undefined>
Global model weights have been loaded...
-----
Now start training...
WARNING:tensorflow:From /usr/local/lib/python3.7/site-packages/tensorflow/python
/ops/math_ops.py:3066: to_int32 (from tensorflow.python.ops.math_ops) is depreca
ted and will be removed in a future version.
Instructions for updating:
Use tf.cast instead.

```

```

binbin.xue@ws-4gpu-4: ~/Client3 Docker package
File Edit View Search Terminal Help
WARNING:tensorflow:From /usr/local/lib/python3.7/site-packages/tensorflow/python
/framework/op_def_library.py:263: colocate_with (from tensorflow.python.framework
k.ops) is deprecated and will be removed in a future version.
Instructions for updating:
Colocations handled automatically by placer.
Loading global model weights...
2019-05-31 13:01:48.547388: I tensorflow/core/platform/cpu_feature_guard.cc:141]
Your CPU supports instructions that this TensorFlow binary was not compiled to
use: AVX2 FMA
2019-05-31 13:01:48.571188: I tensorflow/core/platform/profile_utils/cpu_utils.c
c:94] CPU Frequency: 3597610000 Hz
2019-05-31 13:01:48.572425: I tensorflow/compiler/xla/service/service.cc:150] XL
A service 0x7e7fb01ed820 executing computations on platform Host. Devices:
2019-05-31 13:01:48.572481: I tensorflow/compiler/xla/service/service.cc:158]
StreamExecutor device (0): <undefined>, <undefined>
Global model weights have been loaded...
-----
Now start training...
WARNING:tensorflow:From /usr/local/lib/python3.7/site-packages/tensorflow/python
/ops/math_ops.py:3066: to_int32 (from tensorflow.python.ops.math_ops) is depreca
ted and will be removed in a future version.
Instructions for updating:
Use tf.cast instead.

```

```

binbin.xue@ws-1864-2: ~/Downloads/gitproject/Federated_averaging/client_server_test
File Edit View Search Terminal Help
(tf_p37) binbin.xue@ws-1864-2:~/Downloads/gitproject/Federated_averaging/client
_server_test/Docker_Packaged_Images/Client2 Docker package$ python3 client_main.p
y 106.1.9.199 5000
Using TensorFlow backend.
Model python file has been received and updated
=====
Instructions,weights and hyper-parameters received from server, now compiling
Loading global model weights...
2019-05-31 14:01:37.476187: I tensorflow/core/platform/cpu_feature_guard.cc:141]
Your CPU supports instructions that this TensorFlow binary was not compiled to
use: SSE4.1 SSE4.2 AVX AVX2 AVX512F FMA
2019-05-31 14:01:37.642135: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1
432] Found device 0 with properties:
name: GeForce GTX 1080 Ti major: 1 minor: 1 memoryClockRate(GHz): 1.582
pciBusID: 0000:17:00.0
totalMemory: 10.92GiB freeMemory: 366.50MiB
2019-05-31 14:01:37.811221: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1
432] Found device 1 with properties:
name: GeForce GTX 1080 Ti major: 6 minor: 6 memoryClockRate(GHz): 1.582
pciBusID: 0000:65:00.0
totalMemory: 10.91GiB freeMemory: 9.81GiB
2019-05-31 14:01:37.811376: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1
511] Adding visible gpu devices: 0, 1

```





WoTxR: View WebThingIoTJs's ColorSensor

in RealTime on GearVR with A-Frame on
Samsung Internet VR (svrbrowser)

<http://github.com/samsunginternet/color-sensor-js>

[#LavalVirtual2019](http://is.gd/webxr#)

CC BY-SA 4.0: <http://social.samsunginter.net/@rZR>

THANK YOU

SOSCON2019

SAMSUNG OPEN SOURCE CONFERENCE 2019

