AWS IoT Tutorial

Haoran Li
TA for class CSE 521S, Spring
1/19/2017
Internet-of-Things

Things (Devices)
- Many of them
  - Different Types
  - Isolated Systems

Data and Command
- Sensing the world
- Give Response

Challenge
- United: Connected + Communication
- Smart: Data Analytics + Strategy

Source: https://aws.amazon.com/iot-platform/
http://www.brain-smart.net/smart-brain-health-blog/page/2/#axzz4W4oSp8a6
Solution: AWS IoT

United: Connect + Communication

Smart: Other Cloud Service
Data Storage
Machine Learning

Source: https://aws.amazon.com/iot-platform/
Tutorial: Hello AWS IoT!

Random Integer [1, 100]

LED

>50 : ON
<=50: OFF

AWS IoT

Publish
Subscribe

Forward

Amazon SNS

Source: https://aws.amazon.com/iot-platform/
Step 1: Create a Virtual "Thing"

AWS IoT

Virtual "Thing" / Shadow
Get into AWS Manage Console

- Create your own AWS account
- Sign In IoT Manage Console
  - https://aws.amazon.com/iot/
Create a thing

1. AWS IoT Menu
   - Registry
     - Things ➔ Create

2. Give a name
Basic Interact: Publish

- Using Embedded **MQTT Client** to Test

---

- Check the Things Shadow

---

Shadow Document

**Last update:** Jan 17, 2017 10:24:27 PM -0800

**Shadow state:**

```
1  {
2    "reported": {
3        "Info": "Hello AWS IoT!
4    }
5  }
```
Basic Interact: Subscribe

Devices publish MQTT messages on topics. Subscribe to a topic to view the messages published to it.

Subscription topic:
$saws/things/Test/shadow/update/accepted

Max message capture: 100
Quality of Service: 0

Subscribe to topic

MQTT client

$aws/things/Test/shadow/update/accepted

`{  'state':  [    'reported':  {        'Info': 'Hello AWS IoT!'    }  }`
Step 2: Connect a Physical Device

MQTT Tools

Copy

AWS IoT

Virtual “Thing” / Shadow

Certificate

Attach

Policy

1/19/17
Create and get Certificates

- Create Certificates
  - Security ➔ Certificates ➔ Create

- Download Cert Files
  - 1. public & private key
  - 2. thing cert
  - 3. Root CA for AWS
Create Policy and attach it to cert

- Create Policy
- Attach Policy to Certificates
Connect your Device

- Copy certificates to RP2

- Choose your AWS SDK (support MQTT)
  - Node JS
  - Python
  - Java
  - Embedded C

- You can also use third party MQTT tools
  - Python (paho mqtt library)
Some Notes

1. You will need these certification when setting up the TLS1.2 verification

2. You will need the endpoint and port (8883) when connect to AWS IoT Gateway
Publish / Subscribe

- Publish
  - payload = "{"state":{"reported":{"rndnum":50}}}"

- Subscribe

1/19/17
Step 3: Push Button and Publish

Random Integer [1, 100]

AWS IoT
Step 4: Subscribe and Lit up LED

LED

>50 : ON
<=50: OFF

AWS IoT

Online MQTT Client

Virtual “Thing” / Shadow

Publish

Subscribe
Step 5: Combine Them Together

Random Integer [1, 100]

LED

>50 : ON
<=50: OFF

AWS IoT

Publish
Subscribe
More Fancy: SNS services

Simple Notification Service

![Diagram showing the interaction between a Raspberry Pi, a mobile phone, and an email client with Subscribe and Publish actions connected to a cloud service labeled 'Virtual “Thing” / Shadow', and 'My Topic' connected to 'AWS IoT' and 'Amazon SNS'.]
Amazon SNS

Create a Topic
- ARN will be used later

Topic details: LED_Litup

- Topic owner: 401317363811
- Region: us-west-2
- Display name: LED_Litup

Subscriptions

- Create subscription
- Request confirmations
- Confirm subscription
- Other subscription actions

Filter

<table>
<thead>
<tr>
<th>Subscription ID</th>
<th>Protocol</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>arn:aws:sns:us-west-2:401317363811:LED_Litup:9d1e4c16-4316-47c3-a8f1-763c72152...</td>
<td>sms</td>
<td>+1929...</td>
</tr>
<tr>
<td>arn:aws:sns:us-west-2:401317363811:LED_Litup:975dbe42-cde3-4b3a-80fc-a404e6930...</td>
<td>email</td>
<td><a href="mailto:...@gmail.com">...@gmail.com</a></td>
</tr>
</tbody>
</table>
Create a Rule in Amazon IoT

- Add a query to filter your interesting topic (event)

  **Rule query statement**
  ```sql
  SELECT * FROM '$aws/things/RaspberryPi/shadow/update/accepted'
  ```

- Add an Action:
  - Forward this message to SNS
  - Specify Dest ARN
  - Enable Rule
Notification on SMS & Email

AWS Notification Message

Sent by

12:11 AM (1 minute ago)

"state":{"reported":{"rndnum":76}},"metadata":{"reported":{"rndnum":1484719897},"version":380,"timestamp":1484719897}

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support
Recap: Hello AWS IoT!

Random Integer [1, 100]

LED

>50 : ON
<=50: OFF

AWS IoT

Publish

Subscribe

Forward

Amazon SNS

Source: https://aws.amazon.com/iot-platform/
Recap: Amazon IoT Architecture

AWS IoT DEVICE SDK
Set of client libraries to connect, authenticate and exchange messages

AUTHENTICATION & AUTHORIZATION
Secure with mutual authentication and encryption

DEVICE GATEWAY
Communicate with devices via MQTT, WebSockets, and HTTP 1.1

DEVICE SHADOWS
Persistent device state during intermittent connections

REGISTRY
Assign a unique identity to each device

AWS IoT API

AWS SERVICES
With these endpoints you can deliver messages to every AWS service.

APPLICATIONS
Applications can connect to shadows at any time using an API
Be Creative!

- Bunch of Services

- Embedded systems + Cloud Services...

- IoT!
One More Thing: Security

➢ DON’T UPLOAD YOUR PUBLIC KEY!!!

Time to Open Source!
What if... 50,000 AWS Bill!

My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above $350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a $50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at $15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay. I'm not saying I shouldn't pay anything, but this just a crazy amount in context. Amazon knew the account was compromised, that is why they sent an email, they knew the account history and I had only spent $213 the previous month. I almost feel they deliberately let it ride to try to earn more money. Does anyone have any experience with this sort of problem?
Pointers

- Amazon IoT
  - [http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html](http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html)

- Amazon SNS
  - [http://docs.aws.amazon.com/sns/latest/dg/welcome.html](http://docs.aws.amazon.com/sns/latest/dg/welcome.html)

- AWS Resource list for course projects

- Apply for $40 credits for Amazon AWS
  - [https://aws.amazon.com/education/awseducate/apply/](https://aws.amazon.com/education/awseducate/apply/)
Project Requirements

- Run in public cloud

- Difficulty varies for listed candidates - will take difficulty into consideration when grading.

- Will grade based on
  - project difficulty
  - quality and depth of work
  - workload distribution among team members

- Milestones: proposal, demo1, demo2, final demo, report.

- Start early! Discuss with us and Dr. Lu