



Connecting IoT to cloud

Darryl Ng

darryl.ng@nus.edu.sg

© 2018 National University of Singapore. All Rights Reserved

AWS IoT



SONOS
THE WIRELESS HIFI SYSTEM

PHILIPS
Healthcare

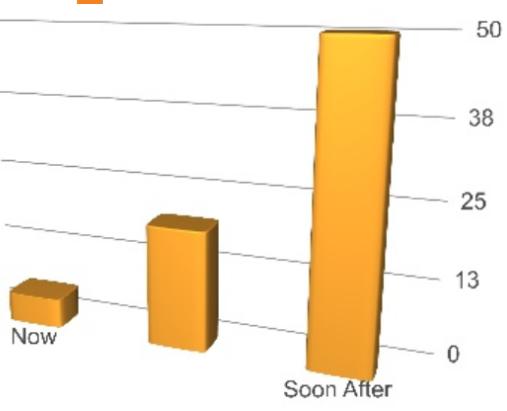
Securely connect one or one billion devices to AWS,
So they can interact with applications and other devices



© 2018 National University of Singapore. All Rights Reserved

In the near future...

Things are becoming connected...



- Today's hype → Tomorrow's normal
- Today's Things → Tomorrow's insights
- Today's technology → Tomorrow's solutions
- Today's definition of "at scale" → Dwarfed by tomorrow's definition
- Today's cost reduction → Tomorrow's growth engine
- Today's confusion → Tomorrow's blue print
- Today's connectivity issues → Solved on the edge

© 2018 National University of Singapore. All Rights Reserved

Internet-of-Things



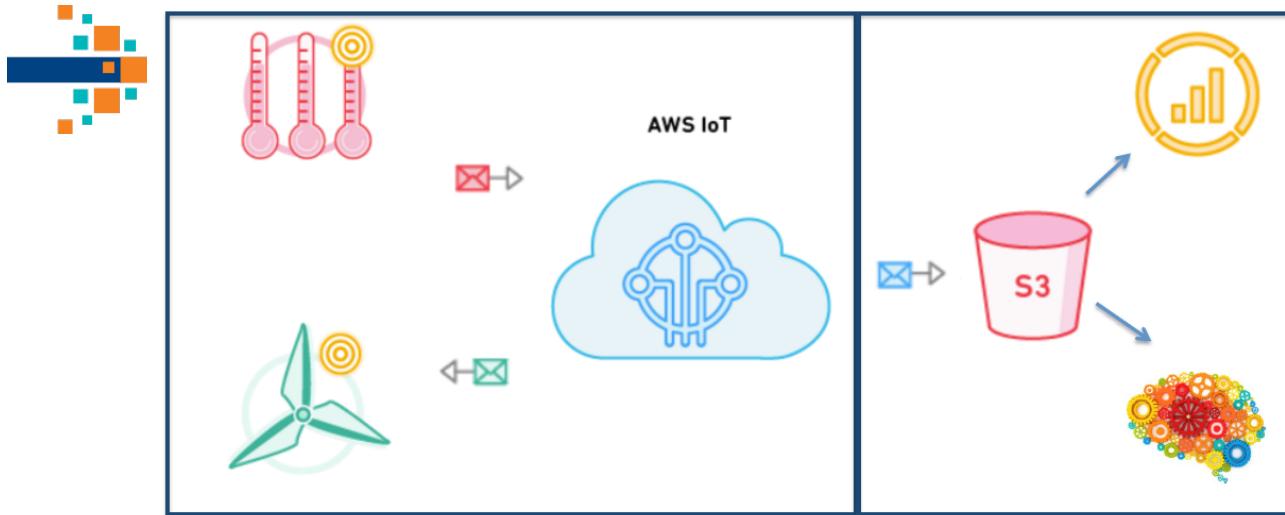
Things (Devices)

- Many of them
 - Different Types
 - Isolated Systems
- Data and Command
 - Sensing
 - Response
- Challenge
 - United: Connected + Communication
 - Smart: Data Analytics + Strategy



© 2018 National University of Singapore. All Rights Reserved

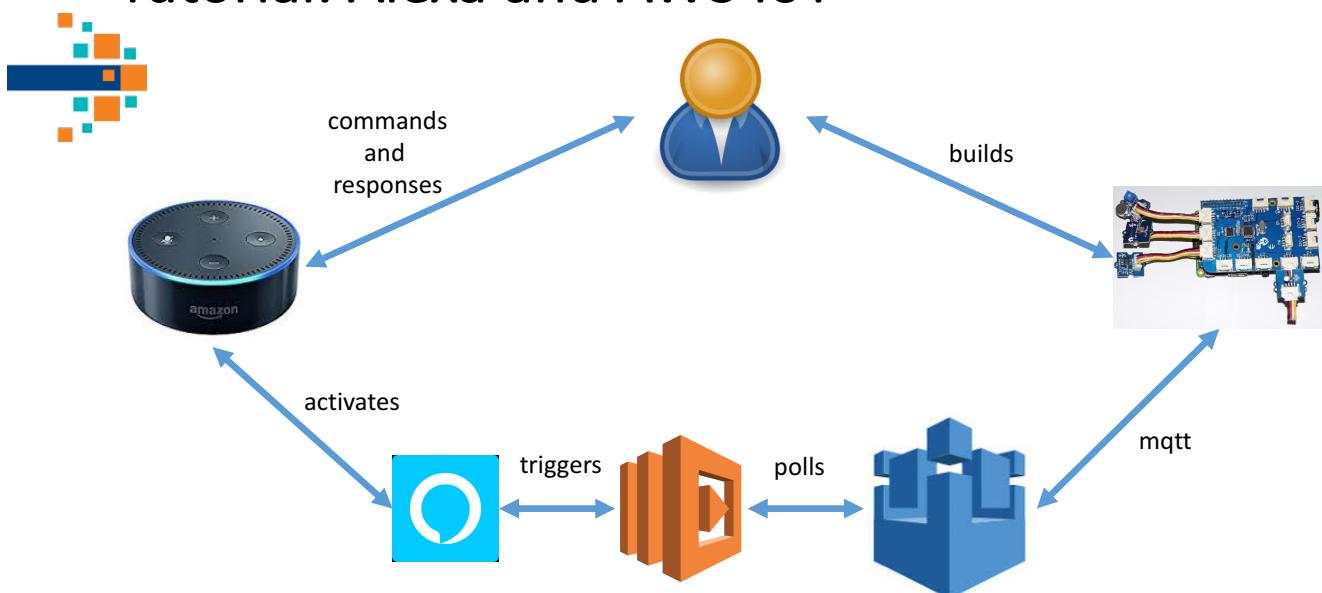
Solution: AWS IoT



- United: Connect + Communicate
- Smart: Storage + Machine Learning

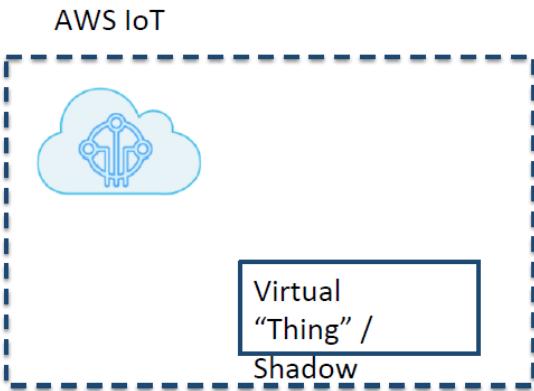
© 2018 National University of Singapore. All Rights Reserved

Tutorial: Alexa and AWS IoT



© 2018 National University of Singapore. All Rights Reserved

Step 1: Create a Virtual “Thing”

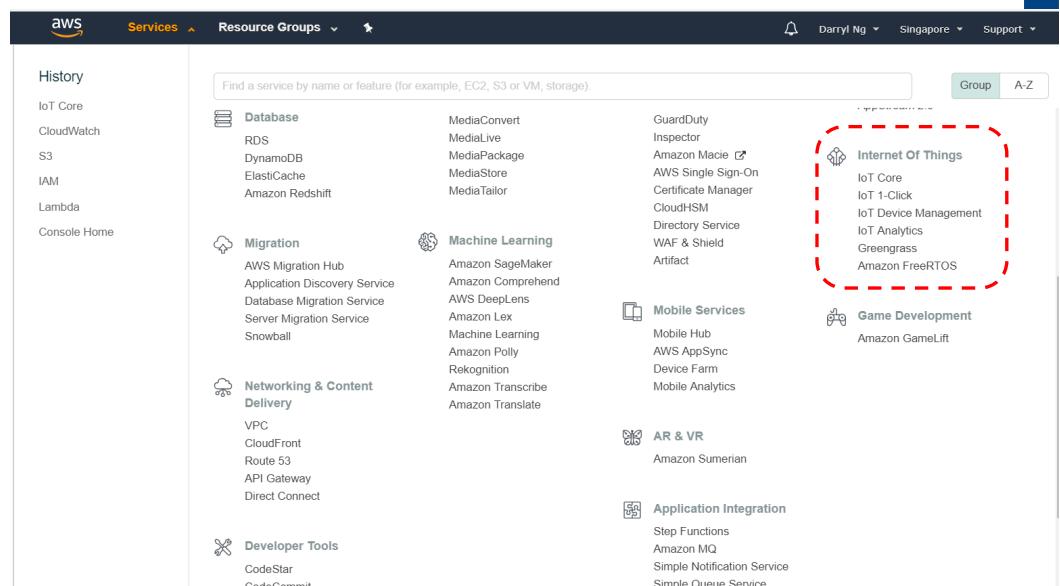


© 2018 National University of Singapore. All Rights Reserved

AWS Management Console



- Create an AWS account
- Sign In to AWS Management Console
 - <https://aws.amazon.com/iot/>



The screenshot shows the AWS Management Console with the Services menu open. The 'Internet Of Things' section is highlighted with a red dashed box. Other visible services include RDS, DynamoDB, ElastiCache, Amazon Redshift, AWS Migration Hub, Application Discovery Service, Database Migration Service, Server Migration Service, Snowball, Amazon SageMaker, Amazon Comprehend, AWS DeepLens, Amazon Lex, Machine Learning, Amazon Polly, Rekognition, Amazon Transcribe, Amazon Translate, Mobile Hub, AWS AppSync, Device Farm, Mobile Analytics, Amazon Sumerian, Step Functions, Amazon MQ, Simple Notification Service, and Simple Queue Service.

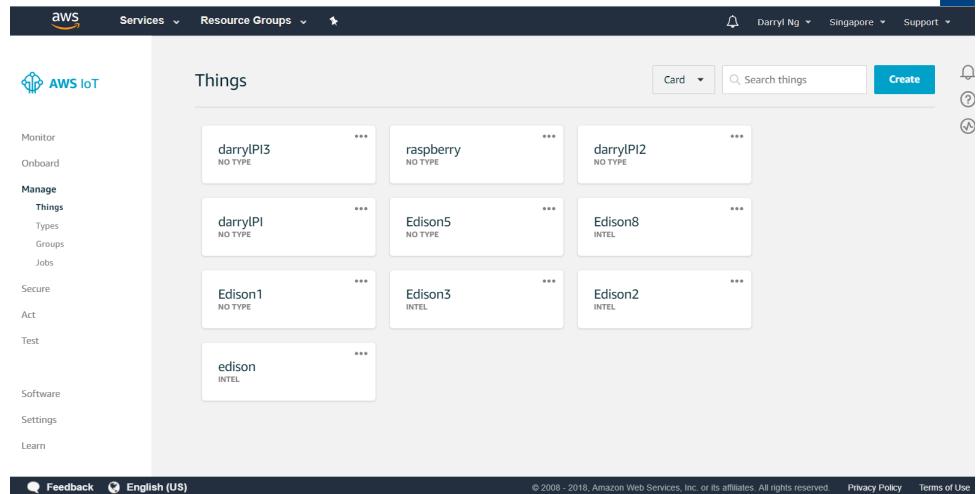
© 2018 National University of Singapore. All Rights Reserved

Create a thing



AWS IoT menu

- Registry
 - Things → Create
- Give a name



The screenshot shows the AWS IoT Things list page. On the left, there's a sidebar with the AWS IoT menu. Under 'Manage Things', it lists 'Types', 'Groups', and 'Jobs'. Below that are 'Secure', 'Act', 'Test', 'Software', 'Settings', and 'Learn' options. The main area is titled 'Things' and shows a grid of registered things. Each thing entry includes the name, type (e.g., NO TYPE, INTEL), and a three-dot menu icon. A 'Create' button is located at the top right of the list.

© 2018 National University of Singapore. All Rights Reserved

Basic Interaction: Publish



Use Embedded MQTT Client to Test



The screenshot shows the AWS IoT Publish interface. It has a 'Publish' section where users can specify a topic and message. The topic is set to '\$aws/things/Test/shadow/update/accepted'. The message content is a JSON payload:

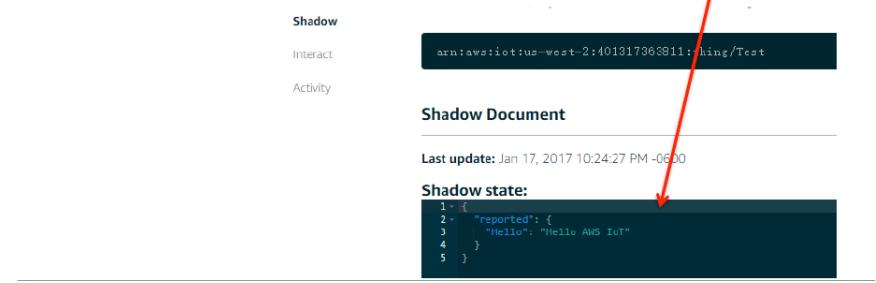
```

1 - { "state": 
2 -   {
3 -     "reported": 
4 -       (
5 -         "Hello": "Hello AWS IoT"
6 -       )
7 -     }
8 -   }
9 -

```

A red box highlights the topic field, and a blue 'Publish to topic' button is visible.

- Use Thing Shadow



The screenshot shows the AWS IoT Shadow interface. It displays the published message in the 'Shadow Document' section. The document shows the state update:

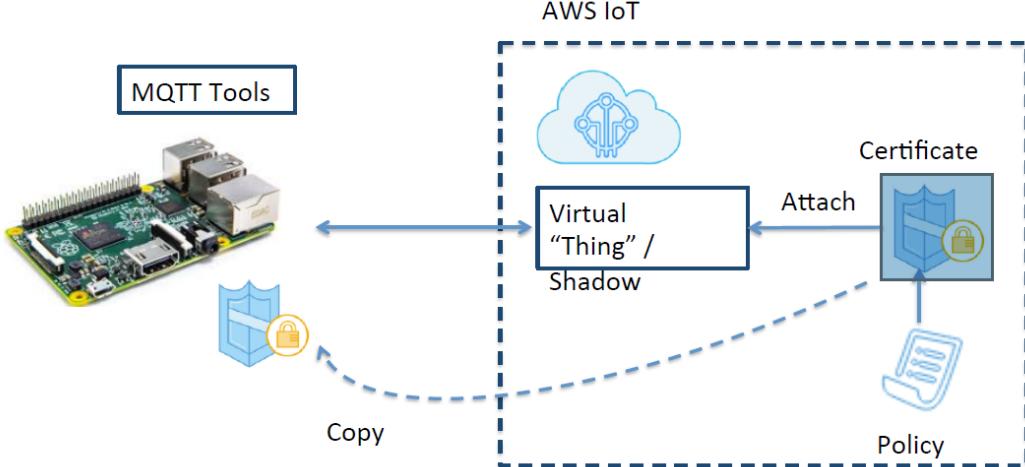
```

Last update: Jan 17, 2017 10:24:27 PM -0600
Shadow state:
1 - {
2 -   "reported": {
3 -     "Hello": "Hello AWS IoT"
4 -   }
5 -

```

© 2018 National University of Singapore. All Rights Reserved

Step 2: Connect a Physical Device

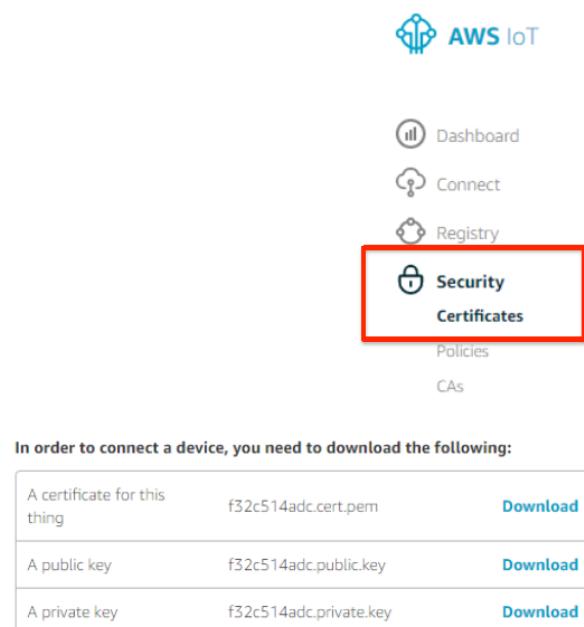


© 2018 National University of Singapore. All Rights Reserved

Certificates and Keys

Create Certificates

- Security → Certificates → Create
- Download Cert Files
 - Public & private key
 - Thing cert
 - Root CA for AWS



In order to connect a device, you need to download the following:

| | | |
|------------------------------|------------------------|--------------------------|
| A certificate for this thing | f32c514adc.cert.pem | Download |
| A public key | f32c514adc.public.key | Download |
| A private key | f32c514adc.private.key | Download |

You also need to download a root CA for AWS IoT from Symantec:
A root CA for AWS IoT [Download](#)

© 2018 National University of Singapore. All Rights Reserved

Create Policy and Attach to certificate


 **Security**

Certificates

Policies

CAs

Certificates15eb5f5a10
ACTIVE

-
- Activate
- Deactivate
- Revoke
- Accept transfer
- Reject transfer
- Revoke transfer
- Start transfer
- Attach policy**
- Attach thing
- Delete

- Attach Policy to Cert

© 2018 National University of Singapore. All Rights Reserved

Connect your Device



- Copy certificates to RPI

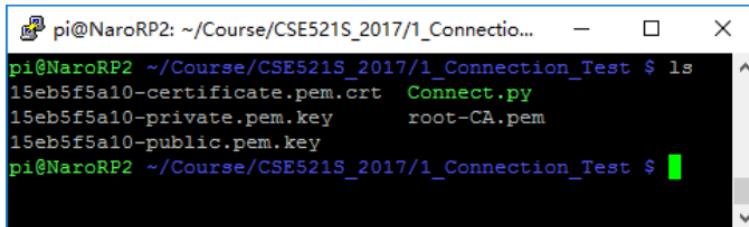
- Choose your AWS SDK (support MQTT)
 - NodeJS
 - Python
 - Java
 - Embedded C
- You can also use 3rd party MQTT tools
 - Python (paho mqtt library)



© 2018 National University of Singapore. All Rights Reserved

Important Notes

- You will need these certification when setting up TLS 1.2 verification



```
pi@NaroRP2: ~/Course/CSE521S_2017/1_Connection_Test $ ls
15eb5f5a10-certificate.pem.crt  Connect.py
15eb5f5a10-private.pem.key      root-CA.pem
15eb5f5a10-public.pem.key
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connection_Test $
```

- You will need the AWS IoT endpoint and port (8883) when connect to AWS IoT

HTTPS

Update your Thing Shadow using this Rest API Endpoint. [Learn more](#)

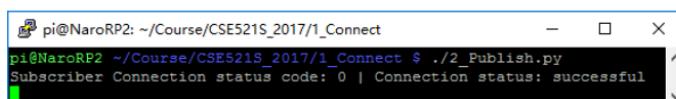
a351pfzlksv6kq.iot.us-west-2.amazonaws.com

/ed

Publish / Subscribe

Publish

➤ payload = "{\"state\":{\"reported\":{\"rndnum\":50}}}"



```
pi@NaroRP2: ~/Course/CSE521S_2017/1_Connect
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connect $ ./2_Publish.py
Subscriber Connection status code: 0 | Connection status: successful
```

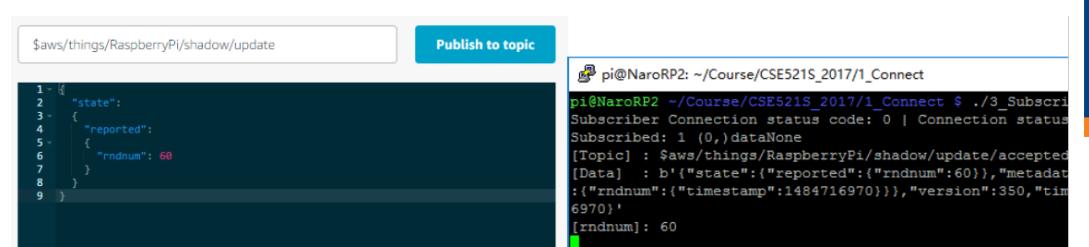
Shadow Document

Last update: Jan 17, 2017 11:18:50 PM -0600

Shadow state:

```
1 + {
2 +   "reported": {
3 +     "rndnum": 50
4 +   }
5 + }
```

- Subscribe



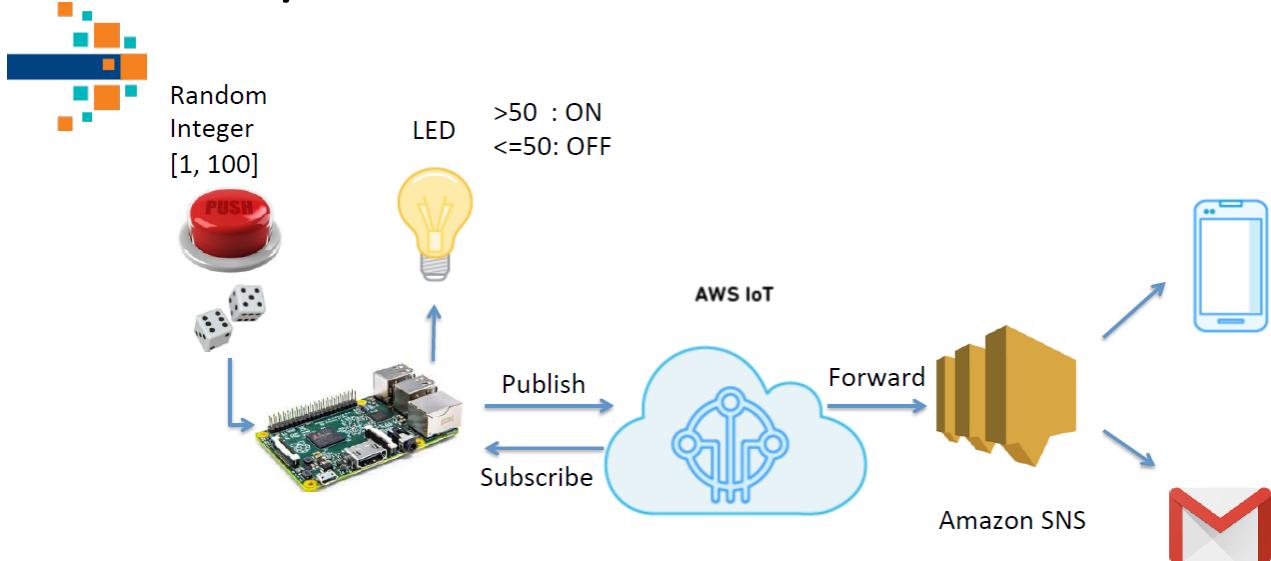
```
$aws/things/RaspberryPi/shadow/update
```

Publish to topic

```
1 - id
2 - "state":
3 - {
4 -   "reported":
5 -   {
6 -     "rndnum": 60
7 -   }
8 - }
```

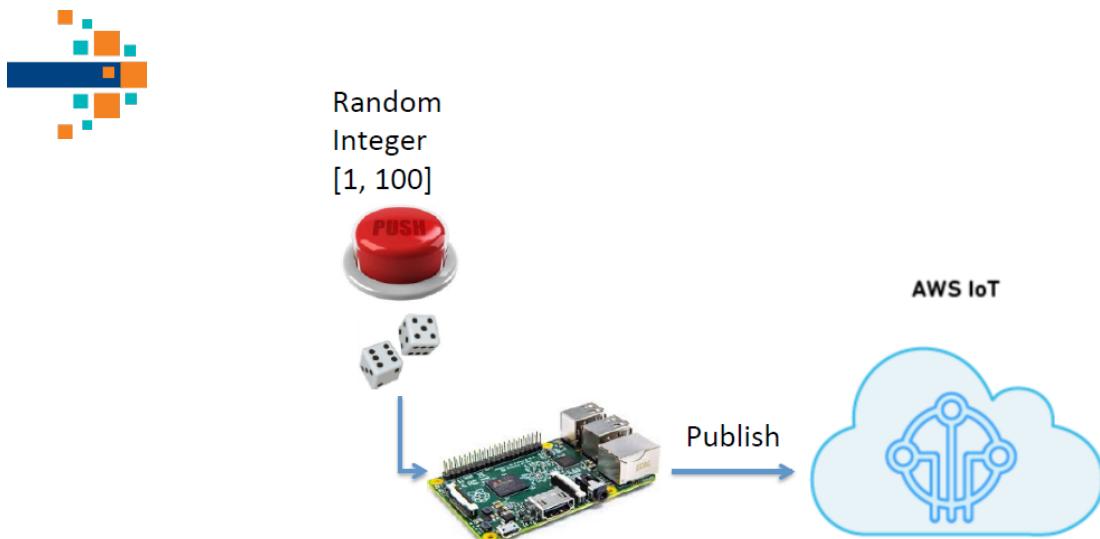
```
pi@NaroRP2: ~/Course/CSE521S_2017/1_Connect
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connect $ ./3_Subscribe
Subscriber Connection status code: 0 | Connection status: successful
Subscribed: 1 (0,)dataNone
[Topic] : $aws/things/RaspberryPi/shadow/update/accepted
[Data] : b'{"state":{"reported":{"rndnum":60}},"metadata":{"rndnum":{"timestamp":1484716970}},"version":350,"time":6970}'
[rndnum]: 60
```

What you can do!!!



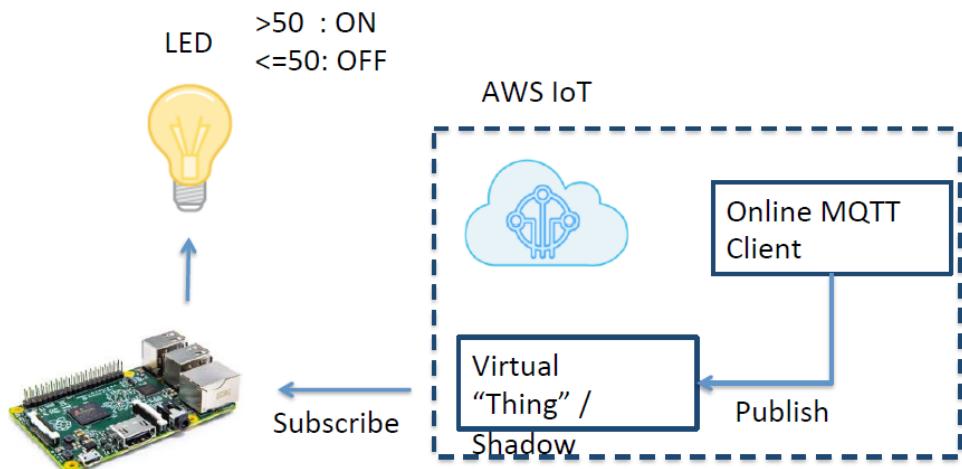
© 2018 National University of Singapore. All Rights Reserved

Push Button and Publish



© 2018 National University of Singapore. All Rights Reserved

Subscribe and Lit up LED

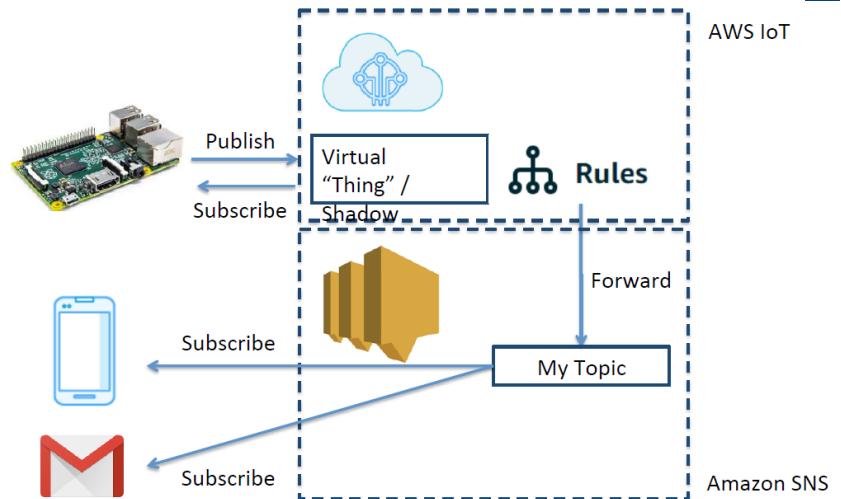


© 2018 National University of Singapore. All Rights Reserved

More Fancy: SNS services



Simple Notification Service



© 2018 National University of Singapore. All Rights Reserved

Amazon SNS



Create a Topic

- ARN will be used

Topic details: LED_Litup

[Publish to topic](#) [Other topic actions ▾](#)

Topic ARN arn:aws:sns:us-west-2:401317363811:LED_Litup

Topic owner 401317363811

Region us-west-2

Display name LED_Litup

Subscriptions

[Create subscription](#)

[Request confirmations](#)

[Confirm subscription](#)

[Other subscription actions ▾](#)

Filter

| <input type="checkbox"/> Subscription ID | Protocol | Endpoint |
|---|----------|----------------------|
| arn:aws:sns:us-west-2:401317363811:LED_Litup:9d1e4c16-4316-47c3-a8f1-763c72152... | sms | +1929[REDACTED] |
| arn:aws:sns:us-west-2:401317363811:LED_Litup:975dbe42-cde3-4b3a-80fc-a404e6930... | email | [REDACTED]@gmail.com |

© 2018 National University of Singapore. All Rights Reserved

Create a Rule in AWS IoT



Add a query to filter your topic (event)

Rule query statement

```
SELECT * FROM '$aws/things/RaspberryPi/shadow/update/accepted'
```

- Add an action:

- Forward message to SNS
- Specify destination ARN
- Enable Rule

[Configure action](#)



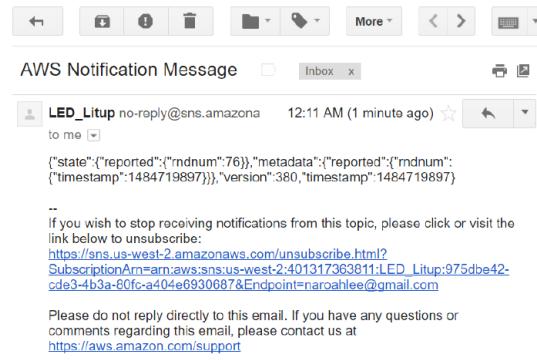
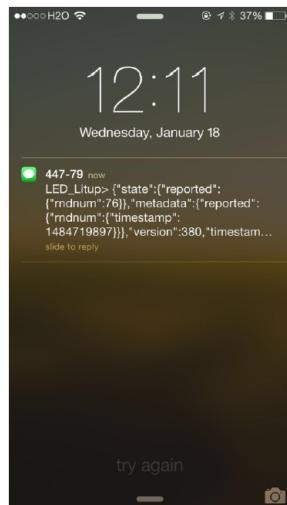
Send a message as an SNS push notification

Rules

ForwardtoSMS
ENABLED

© 2018 National University of Singapore. All Rights Reserved

Notification on SMS & Email

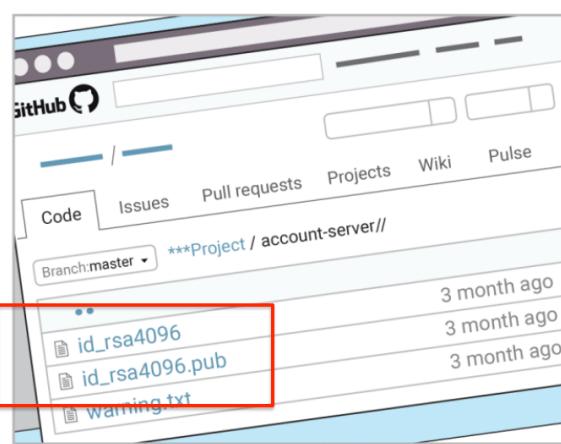


© 2018 National University of Singapore. All Rights Reserved

Important Thing: Security



DON'T UPLOAD YOUR PUBLIC KEY!!!



© 2018 National University of Singapore. All Rights Reserved

What if...


Quora

Ask or Search Quora

Ask Question

Fraud

Amazon Web Services

Amazon.com (product)

Hackers

+3

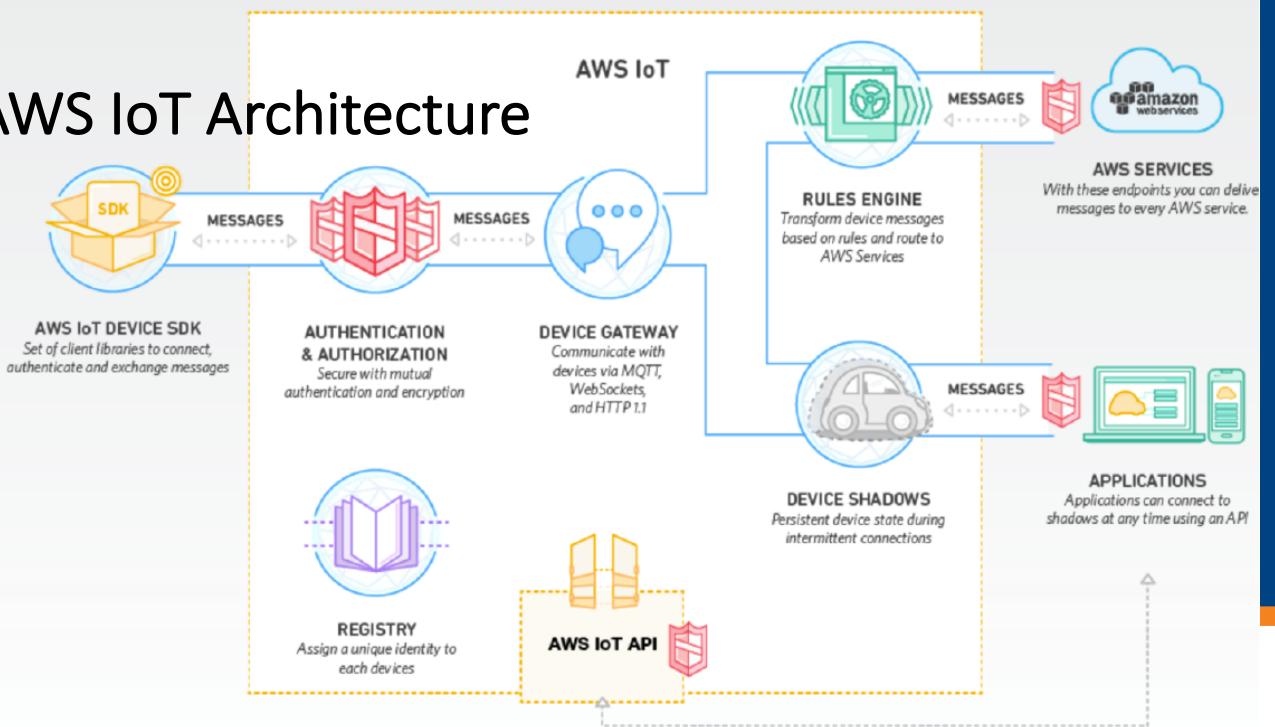


My AWS account was hacked and I have a \$50,000 bill, how can I reduce the amount I need to pay?

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?

© 2018 National University of Singapore. All Rights Reserved

AWS IoT Architecture



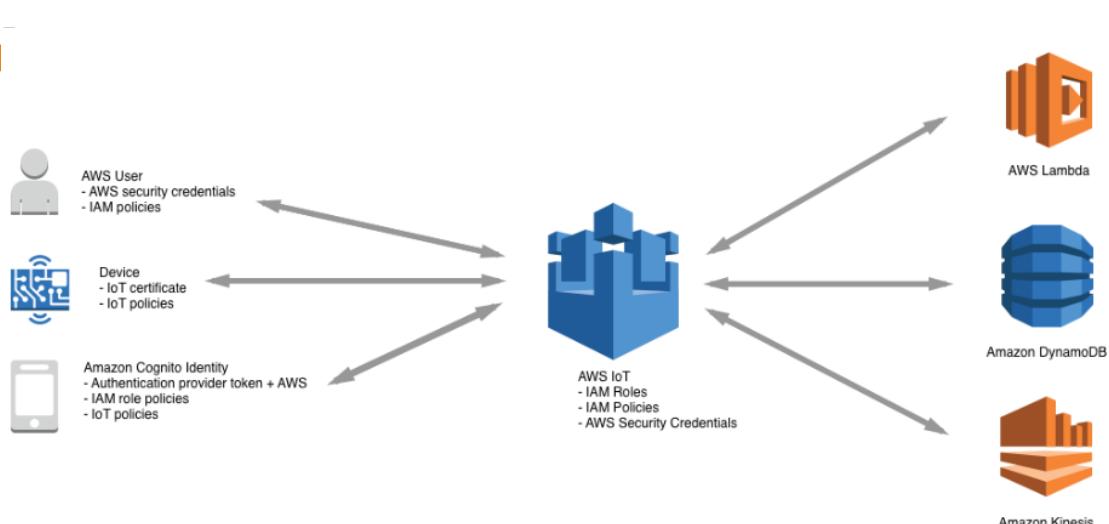
© 2018 National University of Singapore. All Rights Reserved

AWS IoT Authentication

- four types of identity principals
 - X.509 certificates
 - IAM users, groups, and roles
 - Amazon Cognito identities
 - Federated identities

© 2018 National University of Singapore. All Rights Reserved

Security and Identity for AWS IoT



© 2018 National University of Singapore. All Rights Reserved

Security and Identity for AWS IoT

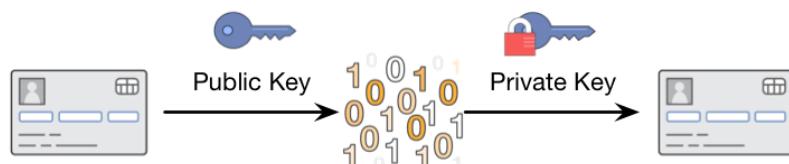
- managing device credentials (X.509 certificates, AWS credentials) on your devices and policies in AWS IoT

- assigning unique identities to each device and managing the permissions for a device or group of devices
- Determining Devices connect using your choice of identity (X.509 certificates, IAM users and groups, Amazon Cognito identities, or custom authentication tokens) over a secure connection according to the AWS IoT connection model

© 2018 National University of Singapore. All Rights Reserved

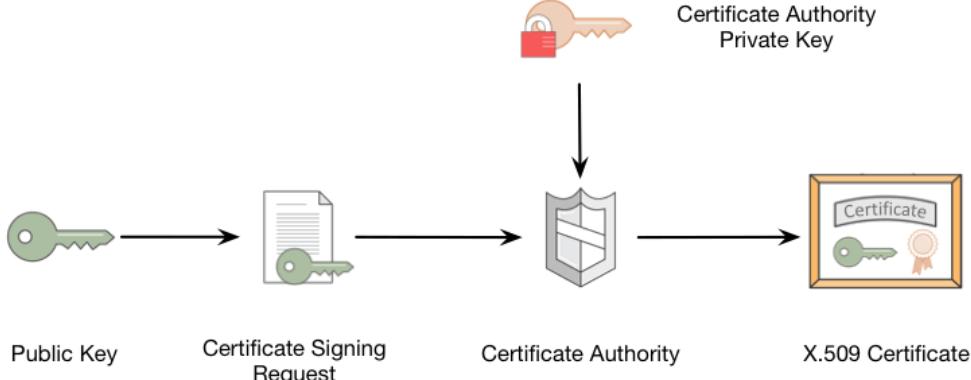
X.509 certificate for identity

- public key cryptography, sometimes called asymmetric cryptography
 - Public key cryptography uses a pair of keys to enable messages to be securely transferred
 - A message can be encrypted using a public key and the only way to decrypt it is to use the corresponding private key:



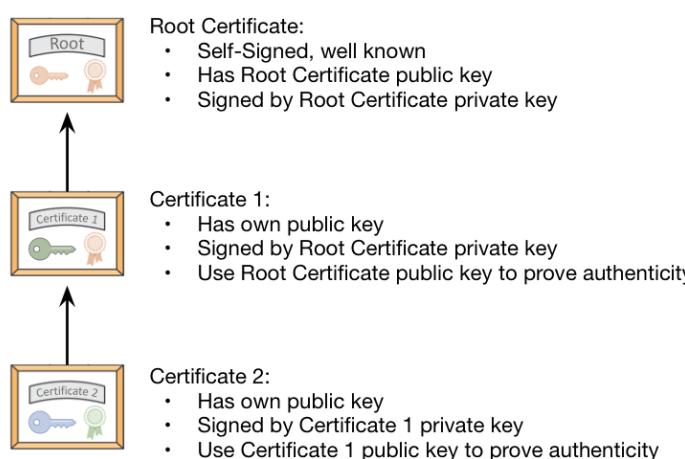
© 2018 National University of Singapore. All Rights Reserved

X.509 certificate for identity



© 2018 National University of Singapore. All Rights Reserved

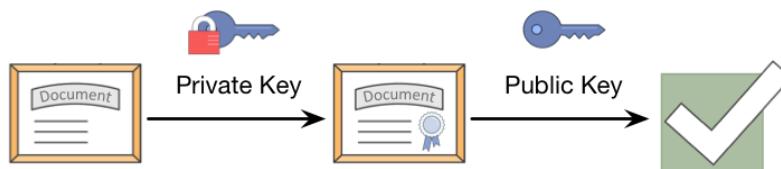
X.509 certificate for identity



© 2018 National University of Singapore. All Rights Reserved

Public Private Key... Continued...

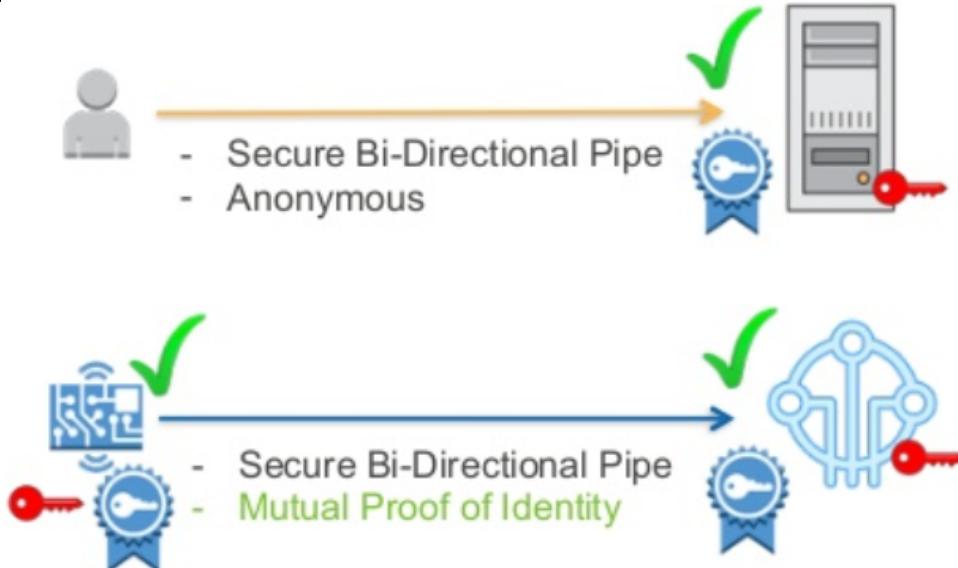
- A key pair is a great way for others to send you secret data
- if you keep your private key secure, anyone with access to the public key can send you an encrypted message that only you can decrypt and read.
- public and private keys also allow you to sign documents.
- a private key is used to add a digital signature to a message. Anyone with the public key can check the signature and know the original message hasn't been altered:



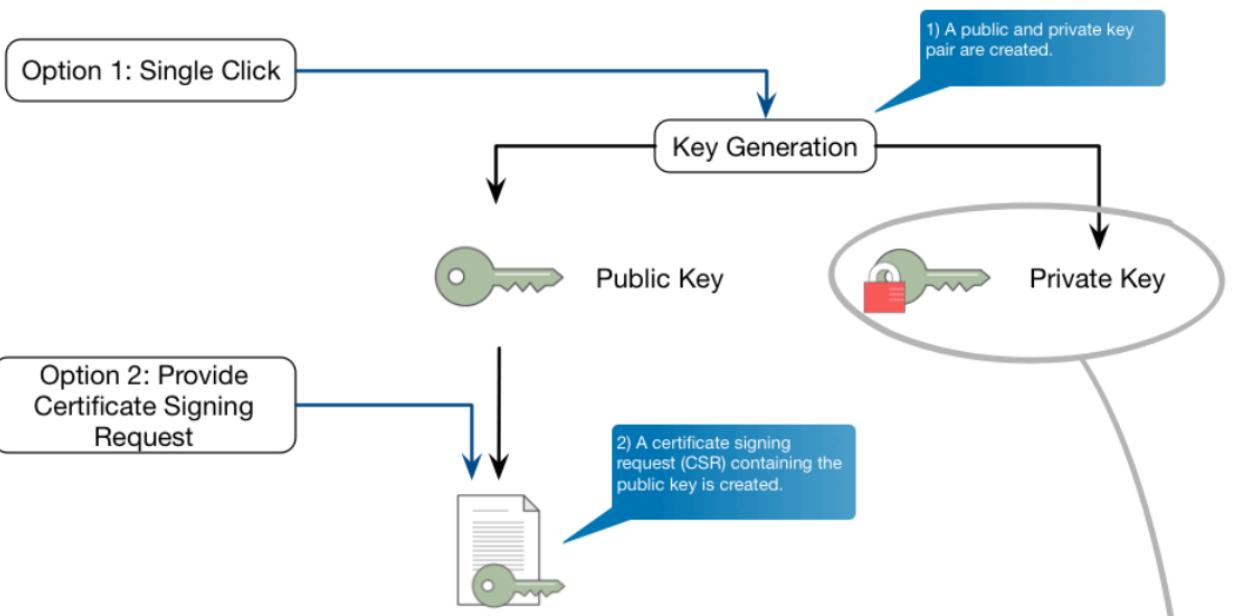
© 2018 National University of Singapore. All Rights Reserved

Securing and Identifying Things: Mutual Auth

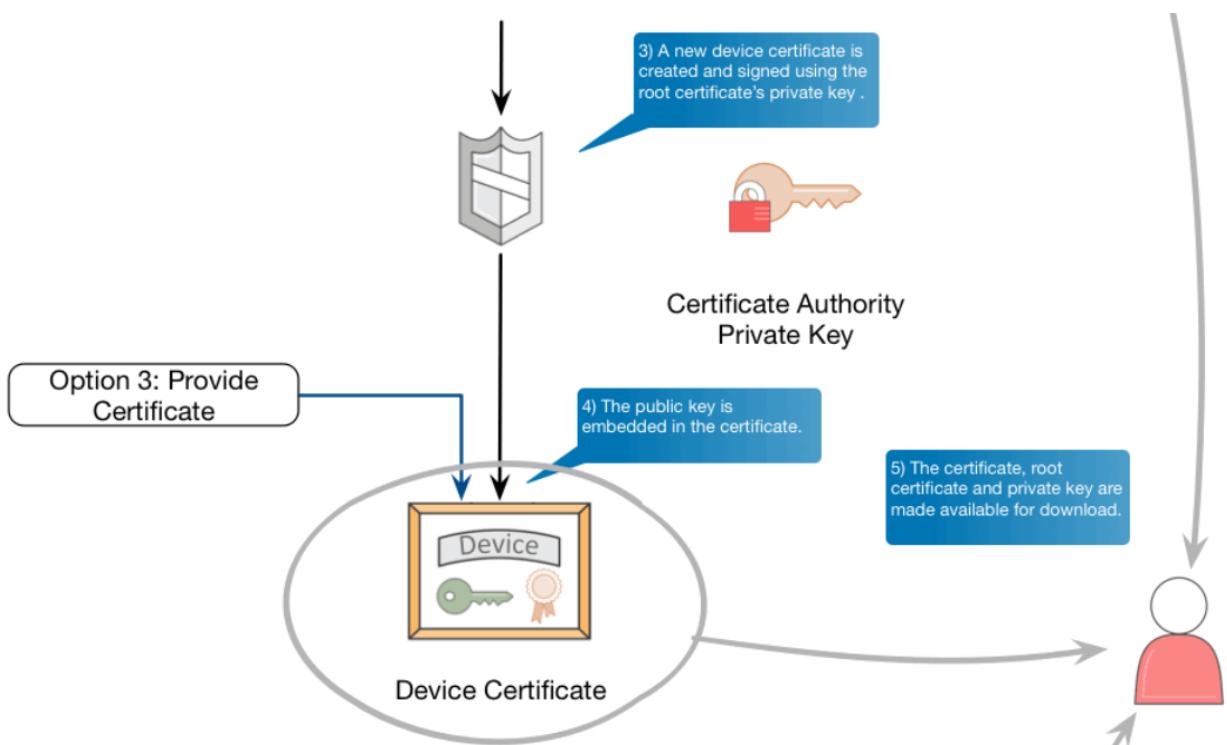
TLS



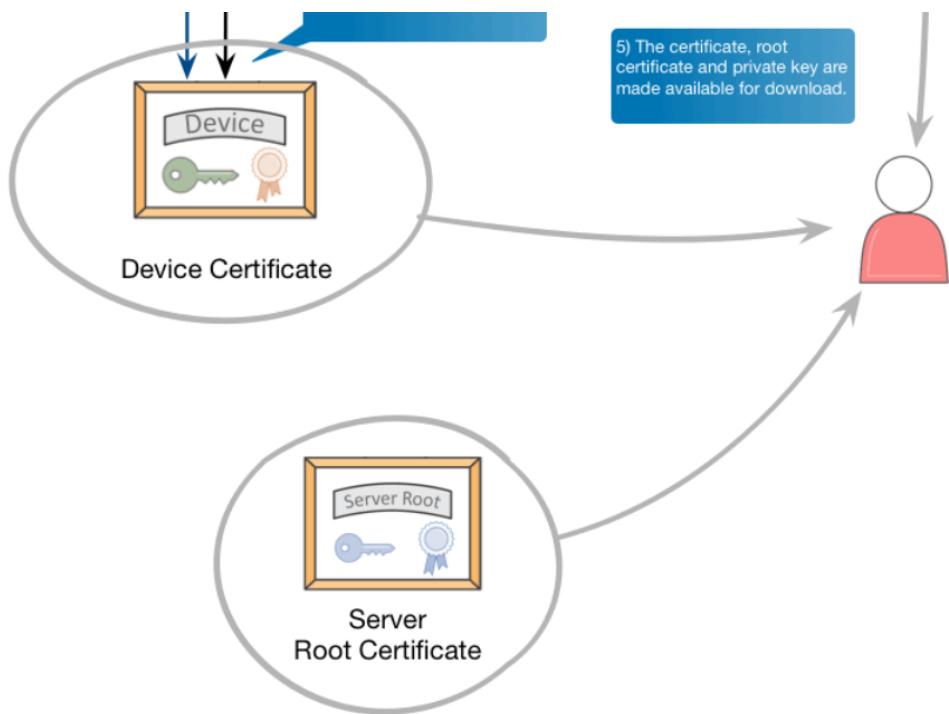
© 2018 National University of Singapore. All Rights Reserved



© 2018 National University of Singapore. All Rights Reserved



© 2018 National University of Singapore. All Rights Reserved



© 2018 National University of Singapore. All Rights Reserved



Message Broker



© 2018 National University of Singapore. All Rights Reserved

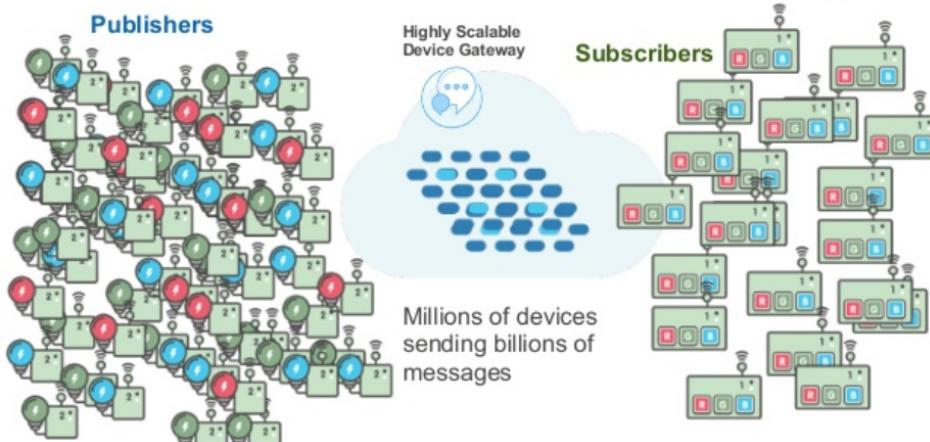
Message Broker (MQTT)

- OASIS standard protocol
- Lightweight, pub-sub, transport protocol
- Application Usage
 - Oil rigs
 - Connected trucks
 - Sensitive and resource-sensitive scenarios

- MQTT vs HTTPS
 - Benchmark
 - 93x faster throughput
 - 11.89x less power consumption to send
 - 170.9x less power consumption to receive
 - 50% less power to keep connected
 - 8x less network overhead
- Source
 - <http://stephendnicholas.com/archives/1217>

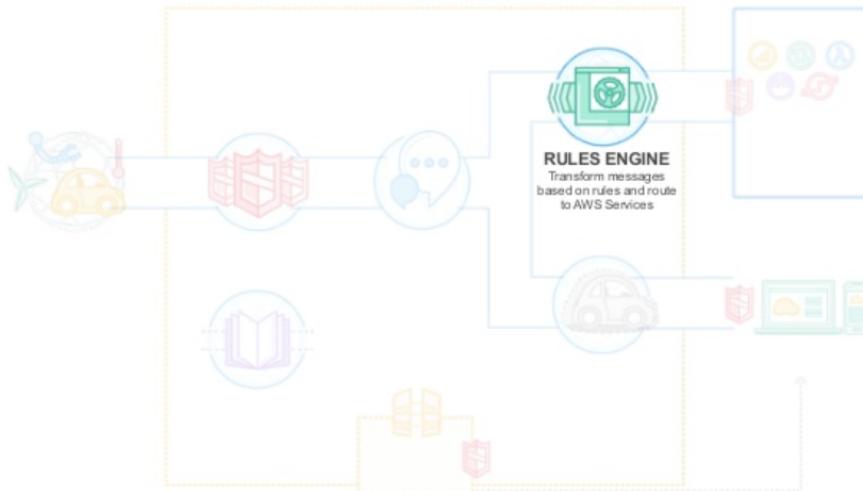
© 2018 National University of Singapore. All Rights Reserved

Message Broker: managed service



© 2018 National University of Singapore. All Rights Reserved

Rules Engine



© 2018 National University of Singapore. All Rights Reserved

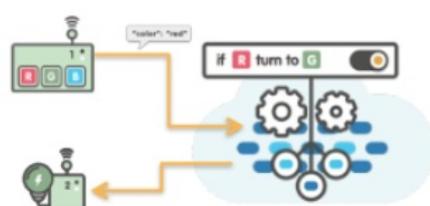
Rules Engine Basics

Simple & familiar syntax

- SQL statement to define topic filter
- Optional WHERE clause
- Advanced JSON support

Functions improvements

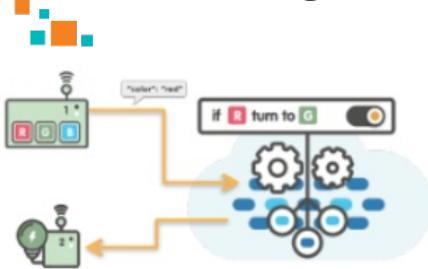
- String manipulation (regex support)
- Mathematical operations
- Context-based helper functions
- Crypto support
- UUID, timestamp, rand, etc.



```
SELECT * FROM 'things/thing-2/color'  
WHERE color = 'red'
```

© 2018 National University of Singapore. All Rights Reserved

Rules Engine's flexibility



```

SELECT *, clientId() as MQTTClientId
FROM 'one/rule'
WHERE
startsWith(topic(2), 'IME33') AND
(state = 'INIT' OR hydro_temp >
surface_temp),
"actions":
[{
"republish": {
"topic": controllers/
${substring(topic(3), 3, 5)}",
}
]

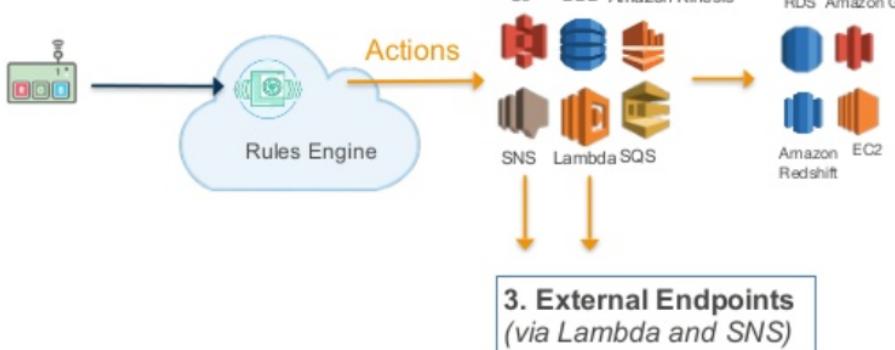
```

- Complex Evaluations
 - Respond to fleet, not just a single unit
 - Dozens of functions available
- Multiple/Simultaneous Actions
 - Sometimes a situation requires you to take many actions

© 2018 National University of Singapore. All Rights Reserved

Rules Engine's integration

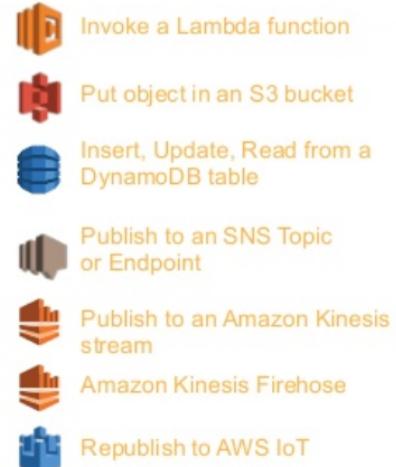
Rules Engine connects AWS IoT to External Endpoints and AWS Services.



© 2018 National University of Singapore. All Rights Reserved

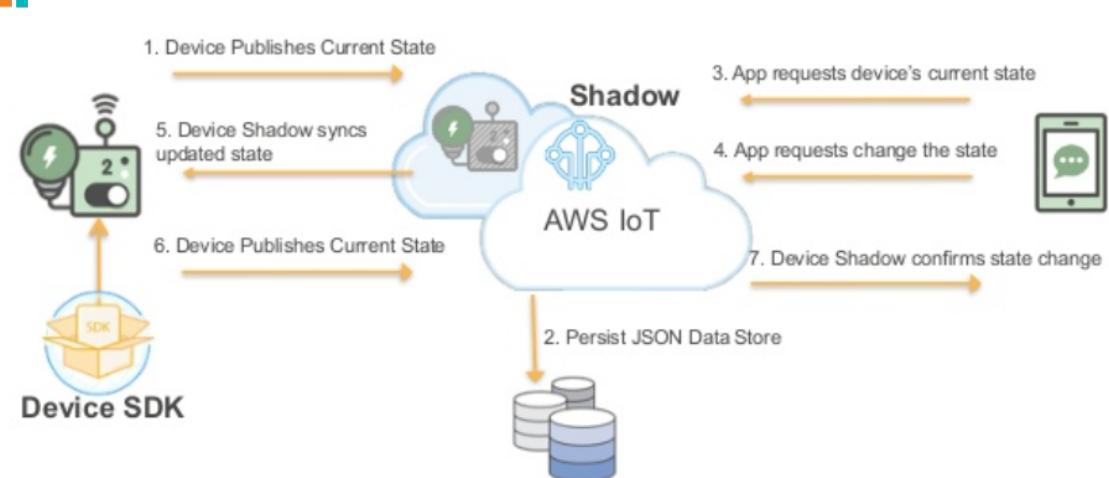
Rules Engine's Actions

- Evaluates inbound messages published into AWS IoT
- Transforms and delivers to appropriate endpoint based on business rules
- External endpoints can be reached via
 - Lambda
 - Simple Notification Services (SNS)



© 2018 National University of Singapore. All Rights Reserved

Thing Shadow and Shadow Flow



© 2018 National University of Singapore. All Rights Reserved

Thing Shadow and Shadow Flow



Report its current state to one or multiple shadows
Retrieve its desired state from shadow

Thing



Shadow reports delta, desired and reported states along with metadata and version

Shadow



Set the desired state of a device
Get the last reported state of the device
Delete the shadow

Mobile App

```
{
  "state": {
    "desired": {
      "lights": { "color": "RED" },
      "engine": "ON"
    },
    "reported": {
      "lights": { "color": "GREEN" },
      "engine": "ON"
    },
    "delta": {
      "lights": { "color": "RED" }
    }
  },
}
```

© 2018 National University of Singapore. All Rights Reserved

AWS IoT Registry



REGISTRY
Identity and Management of
your things

- Static attributes associate to Thing
 - Firmware version
 - Serial Numbers
 - Device Type
 - Device Group
 - Device Description
 - Sensor Description
- Support and Maintenance
 - Reference Manual URL
 - Part # reference
- Reference to external support systems

© 2018 National University of Singapore. All Rights Reserved

Device Management



S3 Holds Versioned Firmware Distributions

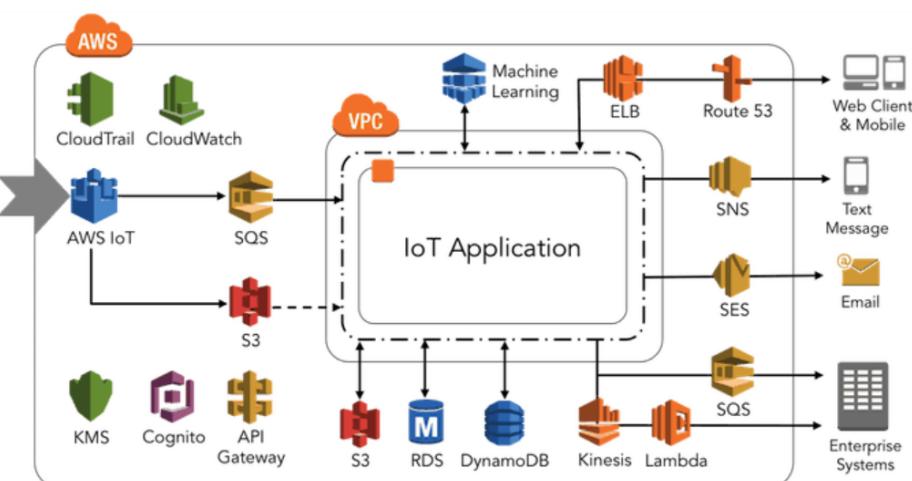
Organize and secure your firmware binaries in S3

Message Broker notifies groups of the fleet using Topic Patterns

Alert the fleet (or part of it) of the update, and send the URL to the S3 download

© 2018 National University of Singapore. All Rights Reserved

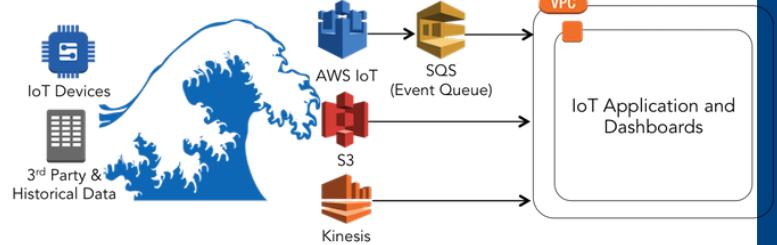
Run IoT solutions at scale on AWS



© 2018 National University of Singapore. All Rights Reserved

BE READY FOR THE DATA TSUNAMI

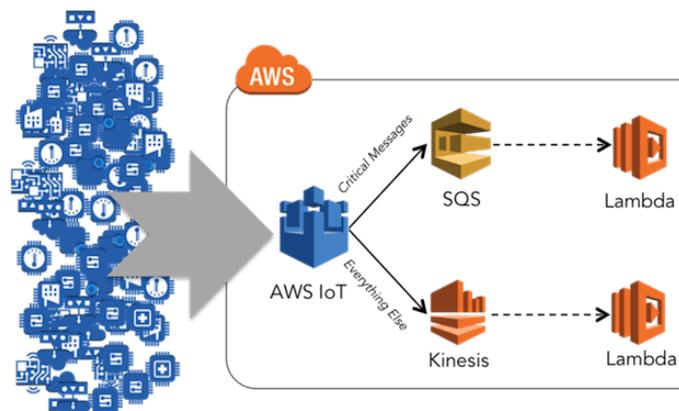
- flood of incoming data comes from
 - sudden surge in business
 - consistent monthly growth
 - malicious attack
- architect your system and AWS components
 - ensure all data is always reliably processed and consistent
- focus on building application intelligence
 - value is created from the data



© 2018 National University of Singapore. All Rights Reserved

PAY ATTENTION TO THE WEAKEST LINK - 1

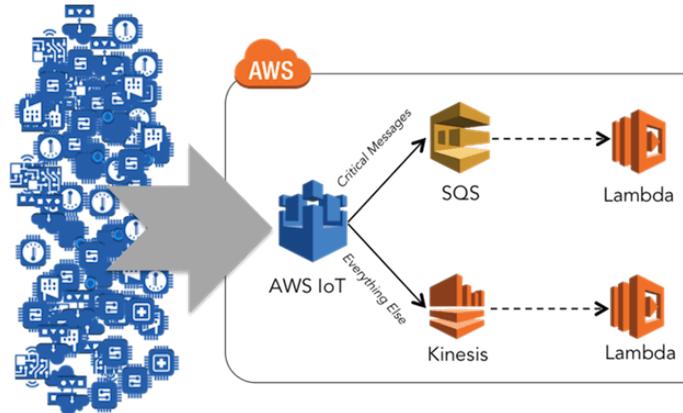
- **AWS IoT Rules** allow you to trigger many different actions upon receipt of a message
- not all services are designed to be used as the single point of entry into the system
- some have behaviors that could prevent all of your data from being processed as desired



© 2018 National University of Singapore. All Rights Reserved

PAY ATTENTION TO THE WEAKEST LINK - 2

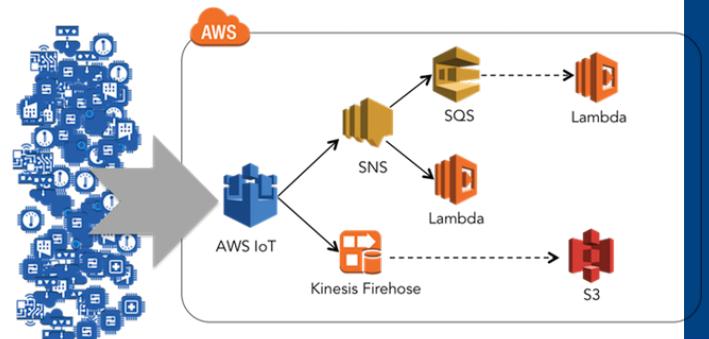
- For example, in high volume applications you should consider buffering or queueing incoming data before invoking downstream services like AWS Lambda, so that in the event of subsequent failures the application still has the ability to recover.
- With unpredictable spikes in data load, in the time it takes for a Lambda function to spin up there could already be 100's of thousands of messages in the pipeline. Going to Lambda directly in this example could result in message loss. But If our data is buffered in Kinesis first, this will give downstream systems time to process any large spikes of incoming data.



© 2018 National University of Singapore. All Rights Reserved

GET IOT DATA INTO A QUEUE AS SOON AS POSSIBLE

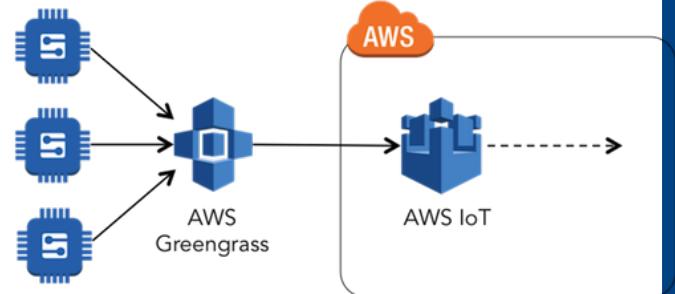
- ensure all incoming data is processed correctly
 - go directly from AWS IoT into a Simple Notification Service (SNS) queue
 - allows AWS fan out your data for processing and ensure the entire flood is reliably captured every time
- get your data somewhere 'safe' prior to processing
 - queue, Amazon Kinesis, Amazon S3, and Amazon Redshift



© 2018 National University of Singapore. All Rights Reserved

THE BEST WAY TO SCALE IS NOT TO SCALE AT ALL

- reduce traffic in the cloud
 - run AWS Greengrass at the edge
- intelligently process and filter data locally
- eliminating the need to send all device data upstream
- need to send 100% of your data all the time
- capture it all, and hold for a limited time, sending to the cloud only when requested or upon certain error conditions
- send a periodic sample or percentage of device data for use by
 - AWS Machine Learning models
 - other cloud analytics tools



© 2018 National University of Singapore. All Rights Reserved

CHOOSE THE INGEST THAT IS BEST

- MQTT is perfect for small payloads of sensor data typical in IoT systems
- MQTT was intended for enabling communications on extremely small embedded devices
 - why use your device's limited power for parsing when it can be offloaded to the cloud?
- Example scenario
 - In a legacy system with log files or XML file dumps, however, it may make more sense to parse the files and send selective values up via MQTT in small chunks.

- key point is that AWS provides several options for data ingest, processing, and storage
 - which should be considered as options for different types of data for use in your IoT solution?
- historical and 3rd party data
 - ingest into Amazon RDS database or via a your own custom REST API backed by Amazon API Gateway
 - Or whether S3 is the answer?

© 2018 National University of Singapore. All Rights Reserved

References

AWS IoT

- <http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>
- <https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html>
- <https://aws.amazon.com/blogs/iot/understanding-the-aws-iot-security-model/>

AWS SNS

- <http://docs.aws.amazon.com/sns/latest/dg/welcome.html>