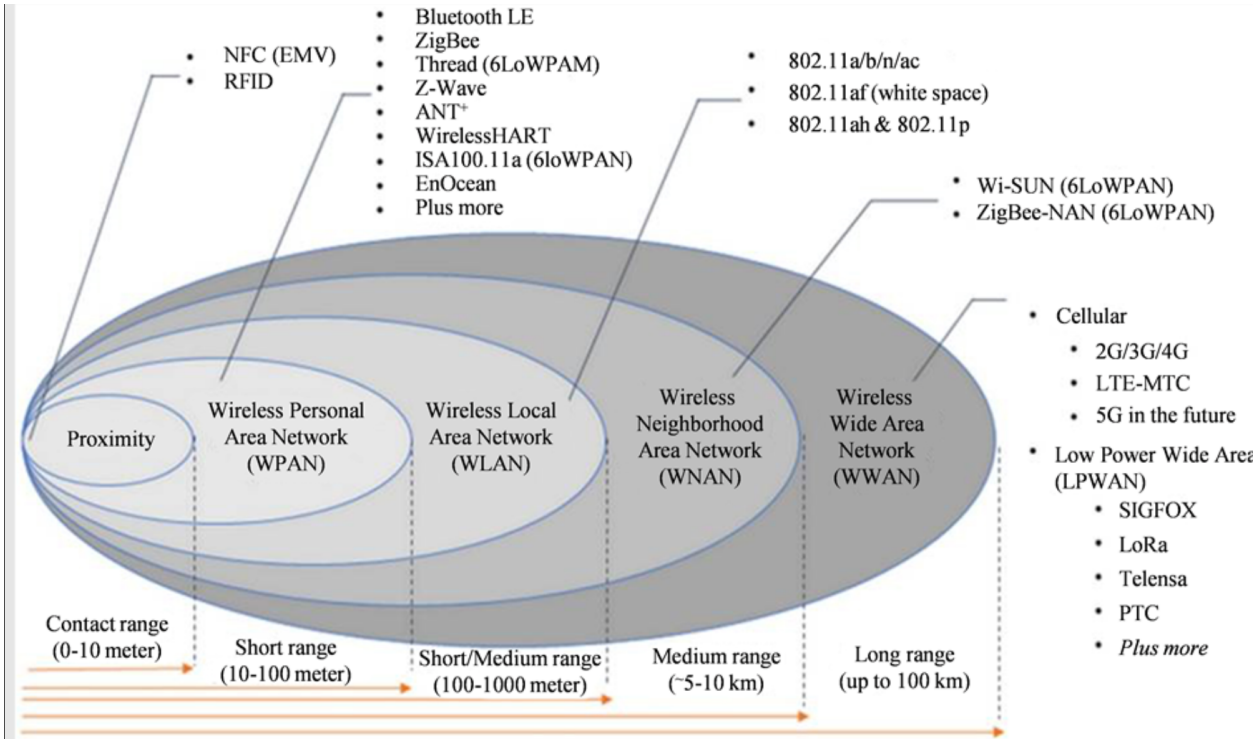
Audrey Long
JHU WEBSEC IOT Assignment
03/30/21

1. IoT Protocols

With the advent of IoT has come the need for protocols that allow different devices to transmit different amounts of data over various distances. Look at this (slightly convoluted) diagram: http://html.scirp.org/file/1-4000110x9.png You'll notice a few protocols that are familiar to you and (probably) many that are new.



2. Deliverables – Part A

1. For each of the 5 ranges at the bottom, select a protocol with which you are unfamiliar. Research the protocol to explain:

I've decided to talk about WWAN

a.) what frequency band does it operate at?

804−967 MHz and 1665−3280 MHz [1]

b.) what transmission (data) rates are supported?

WWAN supports a bitrate of 30 - 50 Mbits/s per user. [2]

c.) what distance is it suitable for?

Up to 120 km

d.) Add more detail, such as typical application, more than what pops up on the first Google search, but don't overdo it!

WWAN networks are essentially traffic which is encapsulated in mobile communication technology also known as mobile broadband. WWAN is a form of wireless network. The larger size of a wide area network compared to a local area network requires differences in technology. Wireless networks of different sizes deliver data in the form of telephone calls, web pages, and streaming video. [4]

2. Now that you're familiar with a new IoT-specific protocol, let's look at them from a security perspective. From the same diagram, choose 2 protocols: one familiar and one unfamiliar Protocol.

a.) Detail any "cyber" attack that is currently known against each of the 2 protocols.

The two protocols I've chosen to talk about are WPAN and WLAN. Intrusions are a common cyber attack on these two network protocols. " the intrusion consists, for an external element, to connect itself to the operator access point and then to be able to penetrate in the network (WLAN, WPAN, ...). This attack can occur in two manners, either coming from the interior of the network or remotely" [5]. Other known similar attacks are MiTM, data capture, intruding access points, eavesdropping, and malicious packet analysis among many others.

b.) Compare (or contrast) how attacks against IoT protocols are like, or different from, traditional network protocols.

Comparing network protocols and IoT protocols there are many differences in regarding data from the attacks from the network layer mentioned above. Another thing that IoT devices need to safeguard against is physical probing with side channel attacks, and differential power analysis to name a few more security considerations.

Please complete both the Alexa Skill and Google Action labs that follow. Remember to take screenshots of important steps – successful output/testing and key configuration items.

3. Alexa Lab 2: Smart Home Skill

This portion of the assignment will leverage some services within AWS that we've encountered before (IAM, Lambda) and others specifically used for integration with IoT devices. For this lab we'll create a virtual Alexa-Enabled Smart Home Lamp, a system to bind the smart lamp to backend resources and test our smart lamp within AWS' IoT Core console.

1. Navigate to the following AWS Hands-on-lab:
https://alexaworkshop.com/en/smart-home.html

2. This lab will require AWS login capability, you can sign up for a student account or a free tier account (both which are later used for the Course Project)

3. Cloud9 environment link:
https://alexaworkshop.com/en/getting-started/create-cloud9-env.html

This link may be helpful to answering some of the following questions
https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html

4. Deliverables – Part B:

1. Annotate the screenshots of important steps – output/testing and key configuration items.

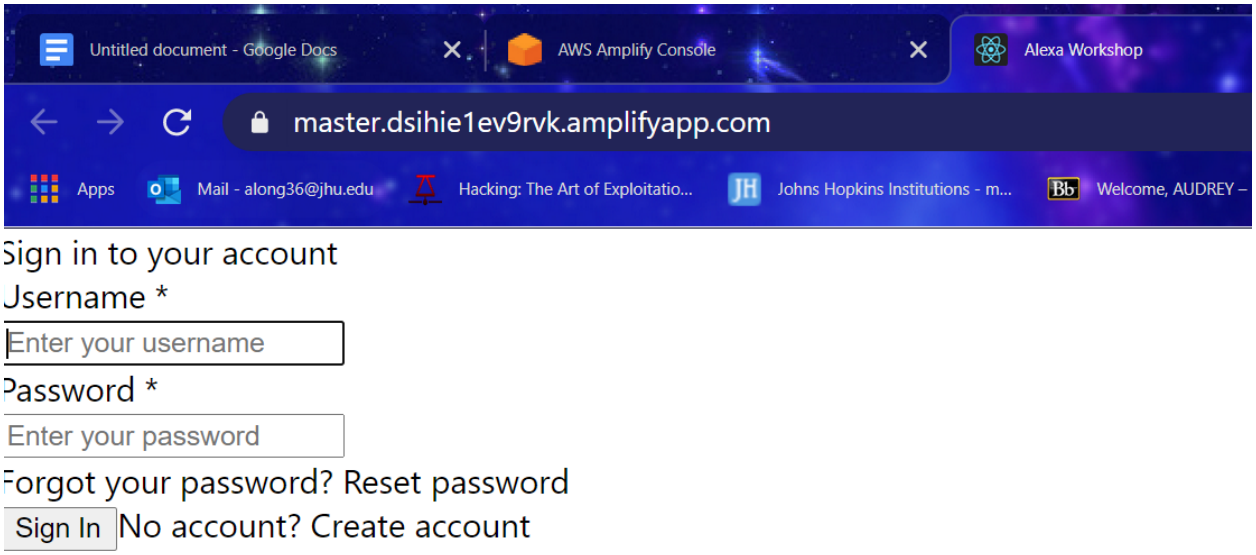


Figure 1: Build Device Binding UI

Figure 2: Build Smart Lamp Simulator

Device-b5y7oiahfvbtfhvwbamcofrbbm-master

Figure 3: Bind Device to User

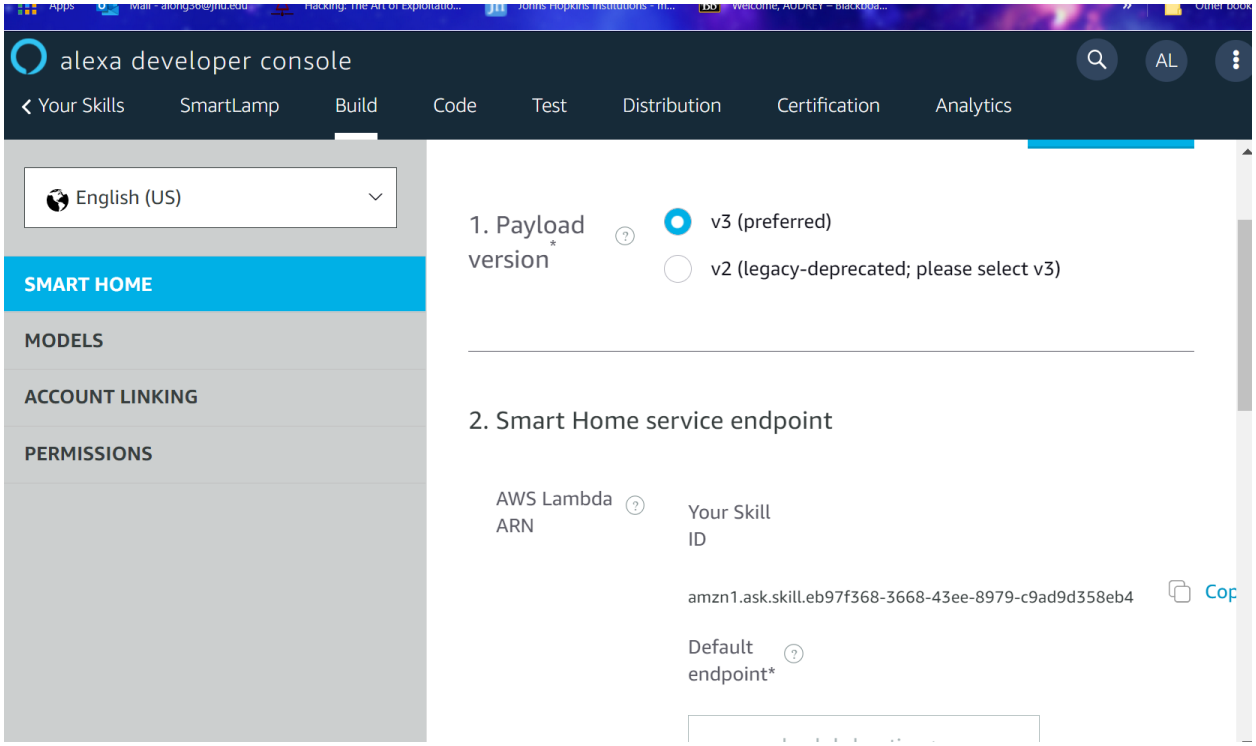


Figure 4: Create Smart Home Skill

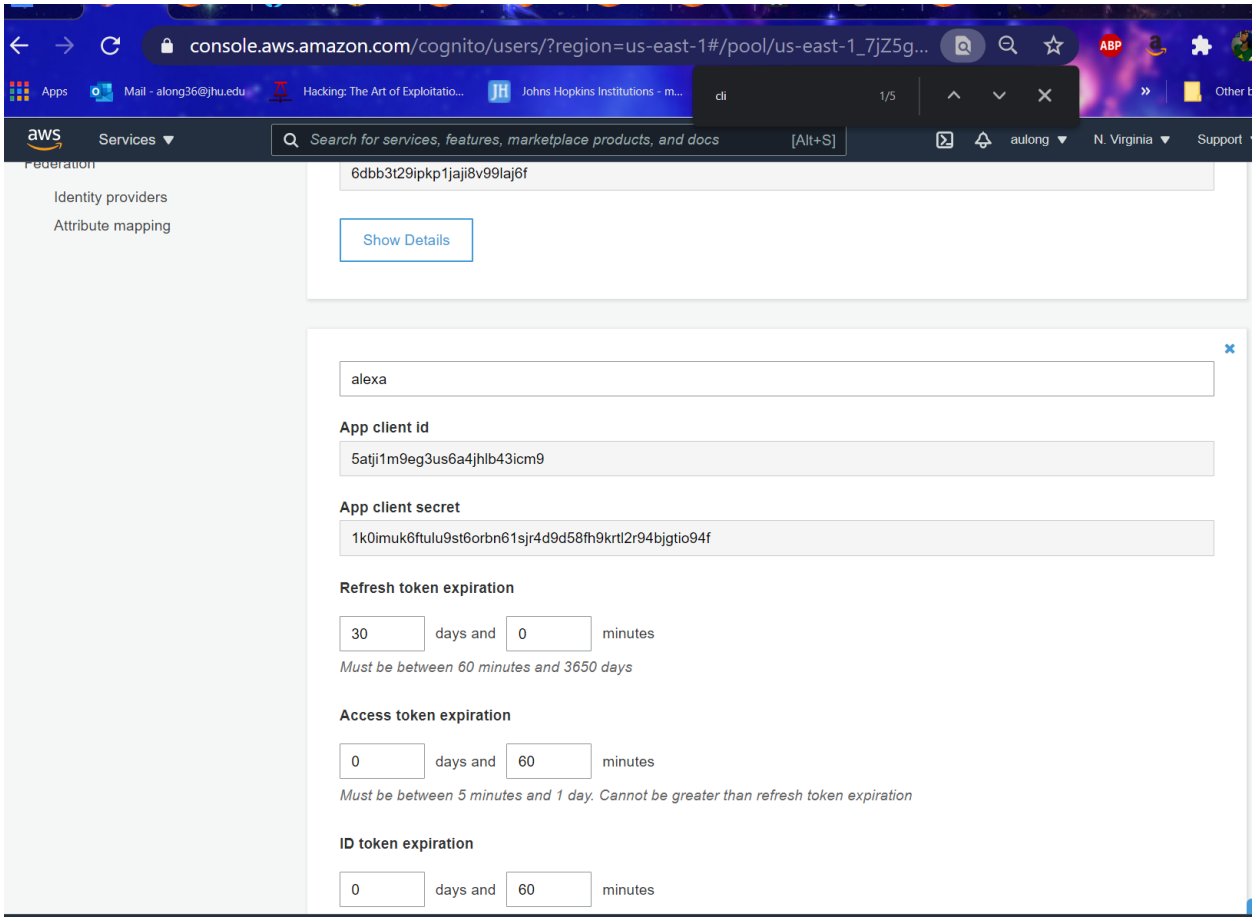


Figure 5: Create Cognito User

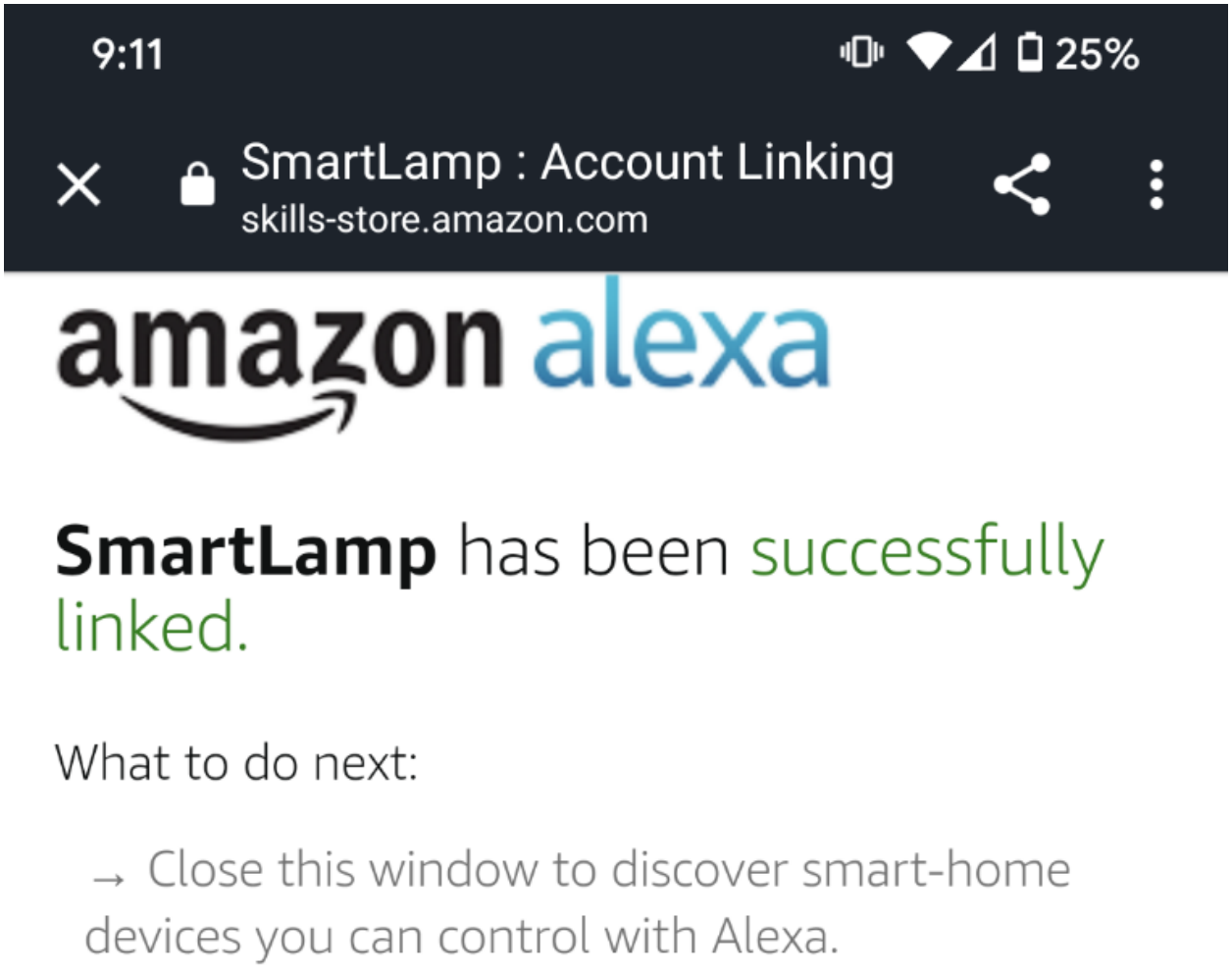

9:11
25%
SmartLamp : Account Linking
skills-store.amazon.com
amazon alexa
SmartLamp has been successfully linked.
What to do next:
→ Close this window to discover smart-home devices you can control with Alexa.

Figure 6: Setup Alexa Account Linking

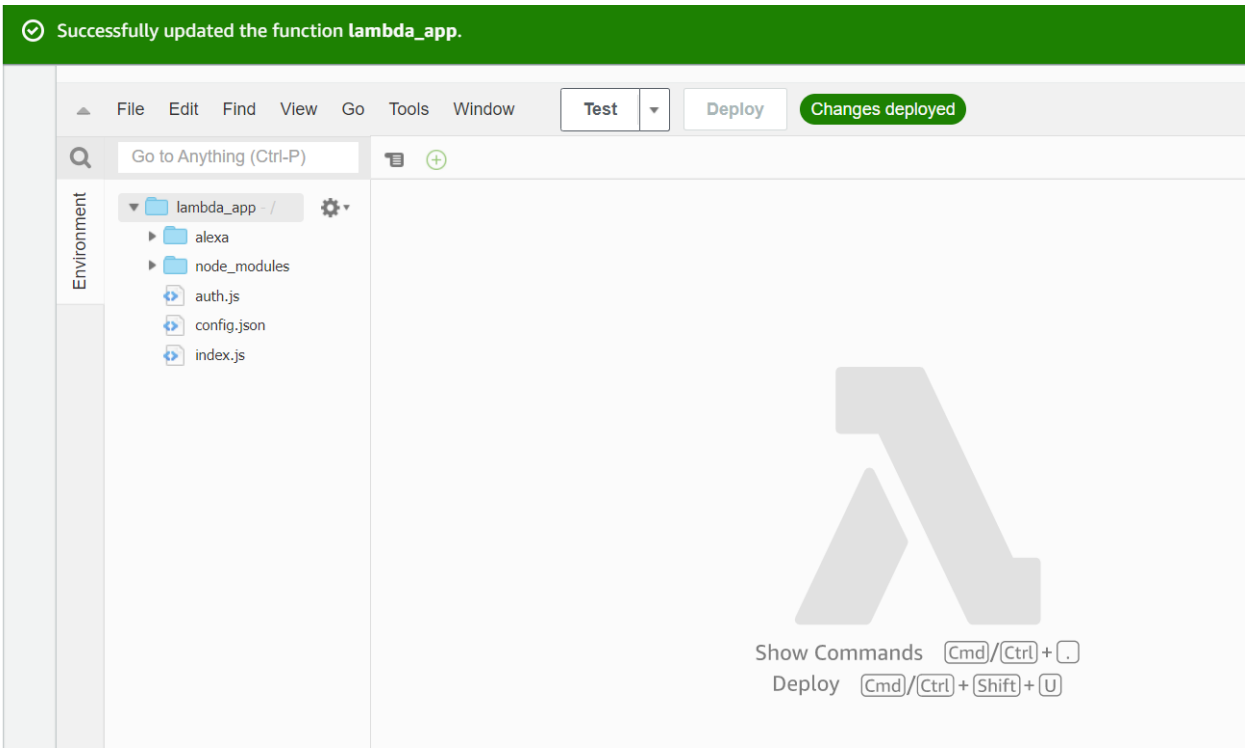


Figure 7: Create Alexa Backend Lambda

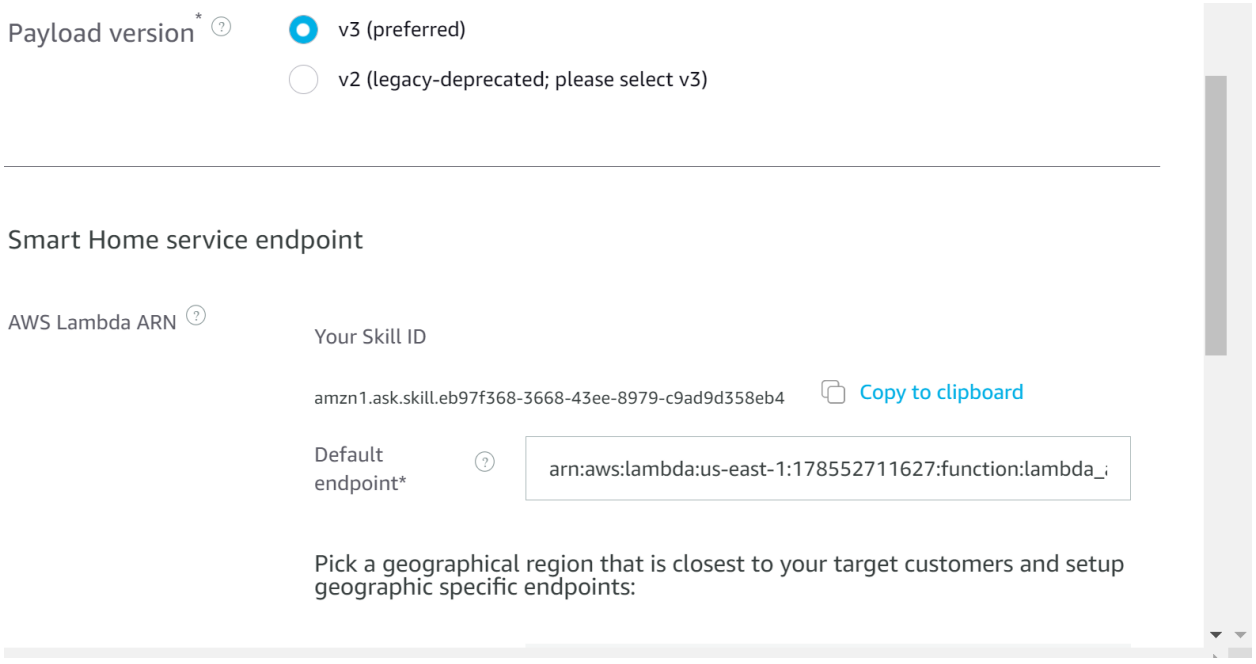
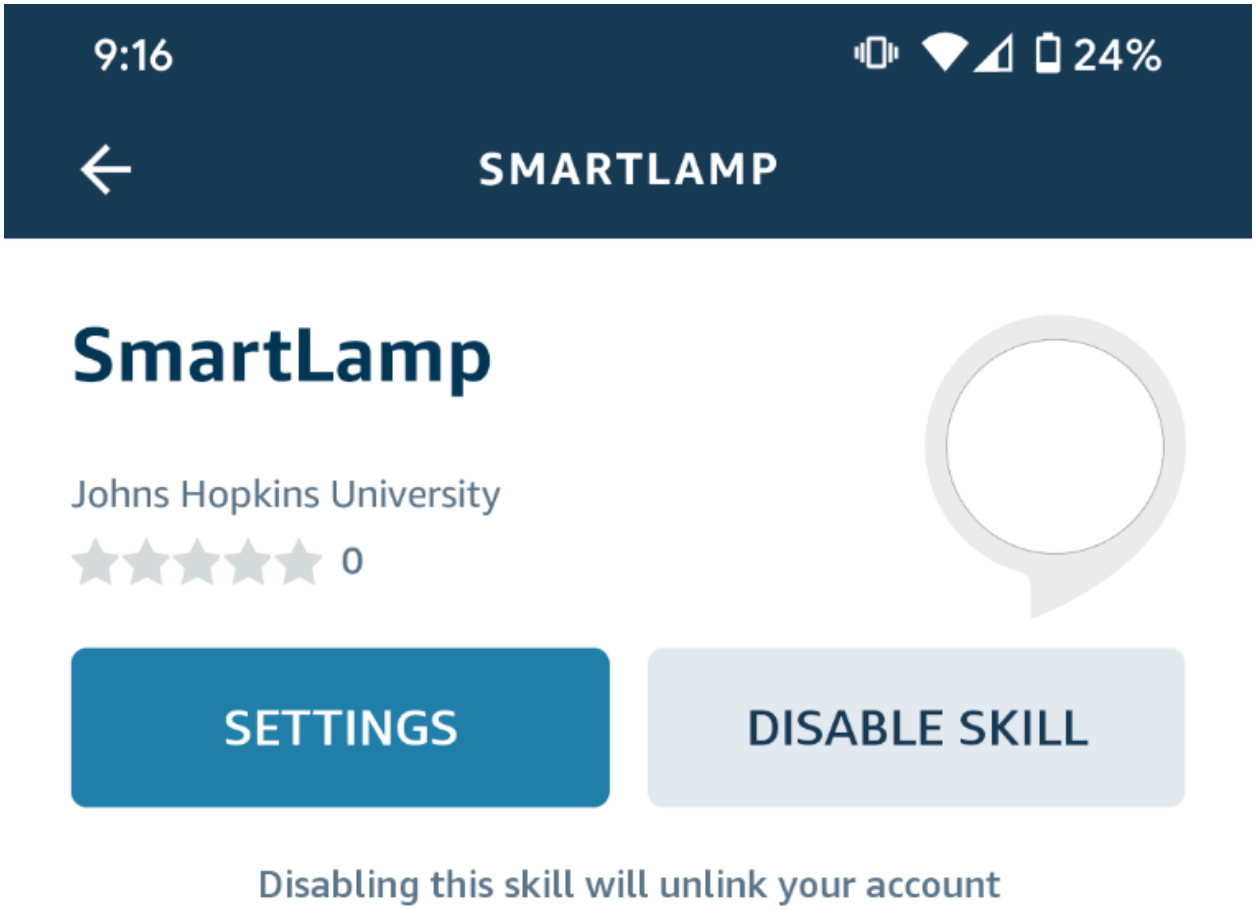


Figure 8: Configure Alexa Skill Endpoint



About this Skill

Note	Smart Home. This skill may share device information with Amazon. Learn more.
Rated	This skill contains dynamic content
Languages	

Figure 9: Discover Smart Home Devices

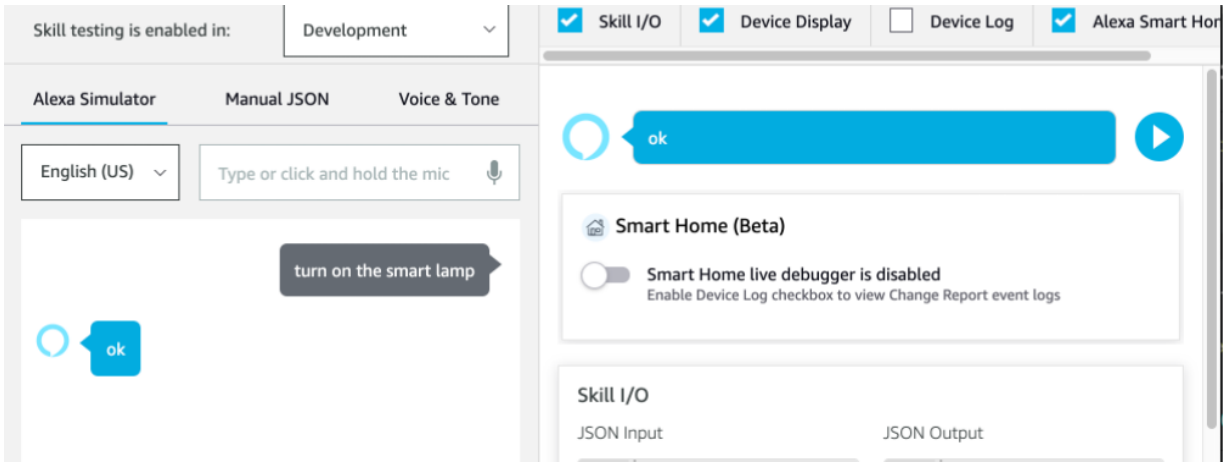


Figure 10: Test Smart Home Skill Endpoint

2. What protocol does AWS use to communicate with linked IoT devices?

AWS supports standard communication protocols such as HTTP, MQTT, web sockets, and LoRaWAN alongside communication utilizing TLS.

3. How does AWS recommend for dealing with IoT vulnerability identification and analysis?

AWS deals with IoT vulnerabilities with the help of IoT device defenders by providing security tools to identify security threats, IoT core provides vulnerability analyzing, monitoring, as well as potential solutions to the issues it has discovered. AWS also provides their security best practices.

4. Describe how a device authenticates to the AWS IoT Core Server.

According to the documentation the IoT core server sends out a self signing cert x.509 which devices authenticate to the server. Then authentication takes place through the TLS protocol by validating the x.509 chain. AWS also provides a certificate chain.

5. What 3 methods does AWS IoT support for client authentication and which option was used within this lab?

The three options within the OAUTH2 flow include: authorization code grant which is what we used in this lab, along with implicit grant, and client credentials.

6. Where is data being stored/queried for our Smart Home lab?

When we set up the data solution for AWS lambda we chose to go the serverless route and all of the data gets stored in RAM. Lambda functions run their own containers on a multi-tenant cluster with RAM and CPU allocated manually.

7. How is data protected while in transit and at rest?

In transit AWS uses TLS and SSL protocols. At rest the storage services will encrypt the data in the service with FIPs standard encryption algorithms.

8. How is key management handled?

Key management in AWS gets handled in the key management service KMS which can be accessed in cloudtrail.

9. AWS encourages enabling monitoring and logging for IoT devices, what services can we use?

Cloud Trail, IoT Core, and AWS Device Defender can be used to enable monitoring, logging, continuous analysis, and threat mitigation.

10. Is there a way to recall all the API calls made to each of the services?

CloudTrail captures all API calls for AWS IoT events.

5. Google Assistant Actions

Remember to take screenshots of important steps – output/testing and key configuration items.

A. Login to your Qwiklabs account and search for: Google Assistant: Qwik Start - Dialogflow

B. Click on the lab and press Start Lab. You will have 75 minutes to complete a lab that is projected to take 30.
Note: The lab specifies a "Quote Generator" but have a little fun and populate the Intent Name, Training Phrases, and Responses with any topics you would like!

6. Deliverables Part C:

1. Annotate the screenshots of important steps – output/testing and key configuration items.

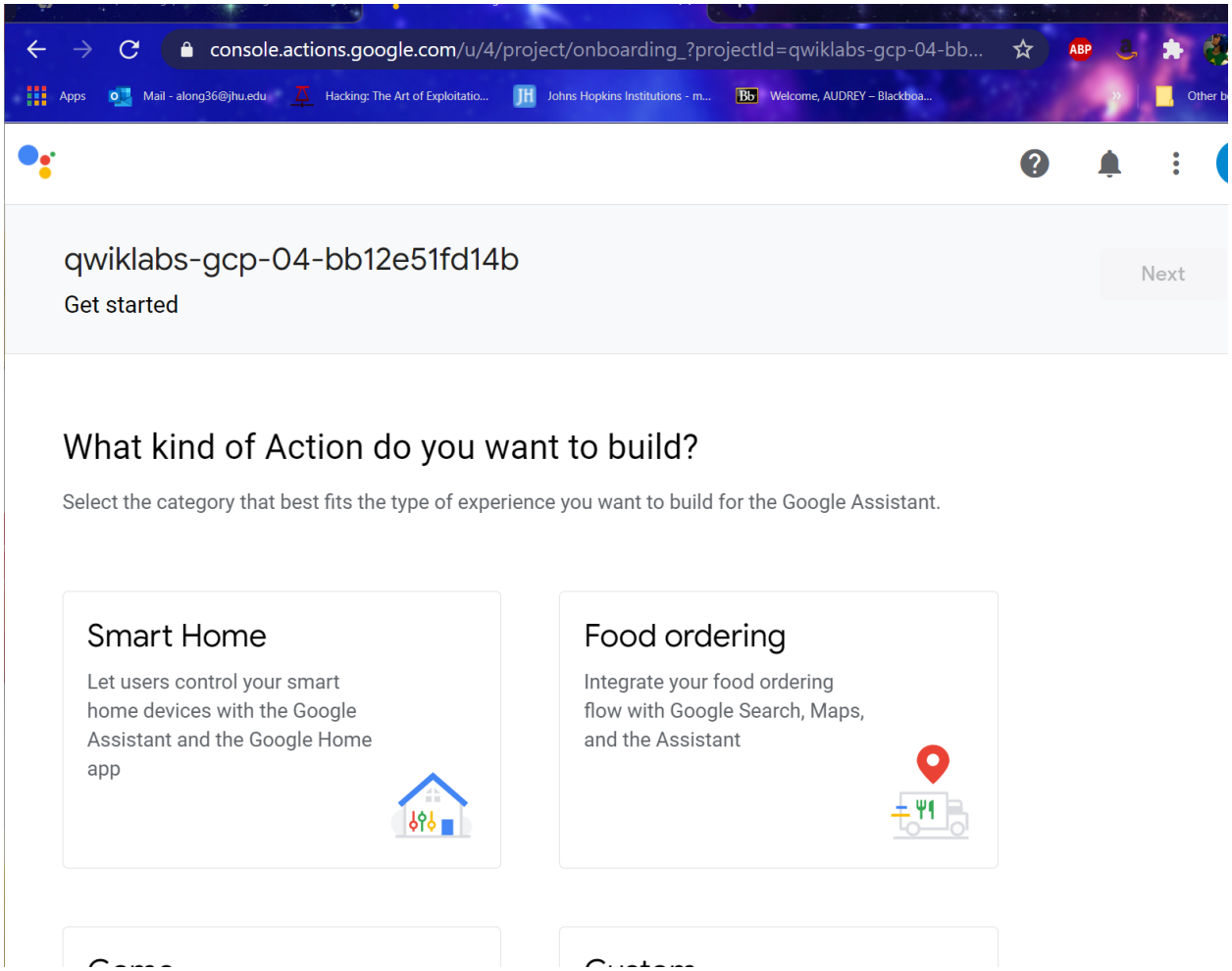


Figure 1: Create an Action project

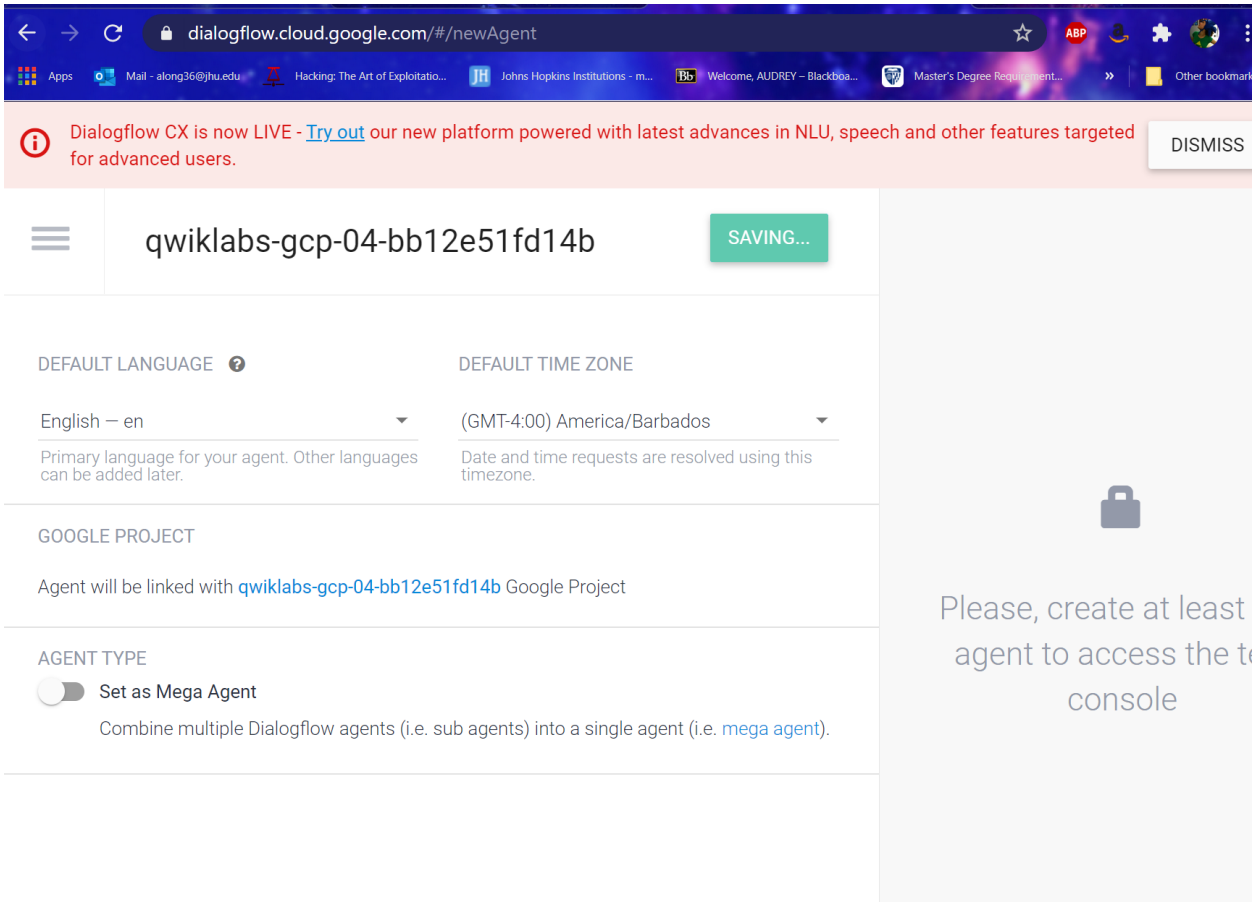


Figure 2: Set up Dialog Flow

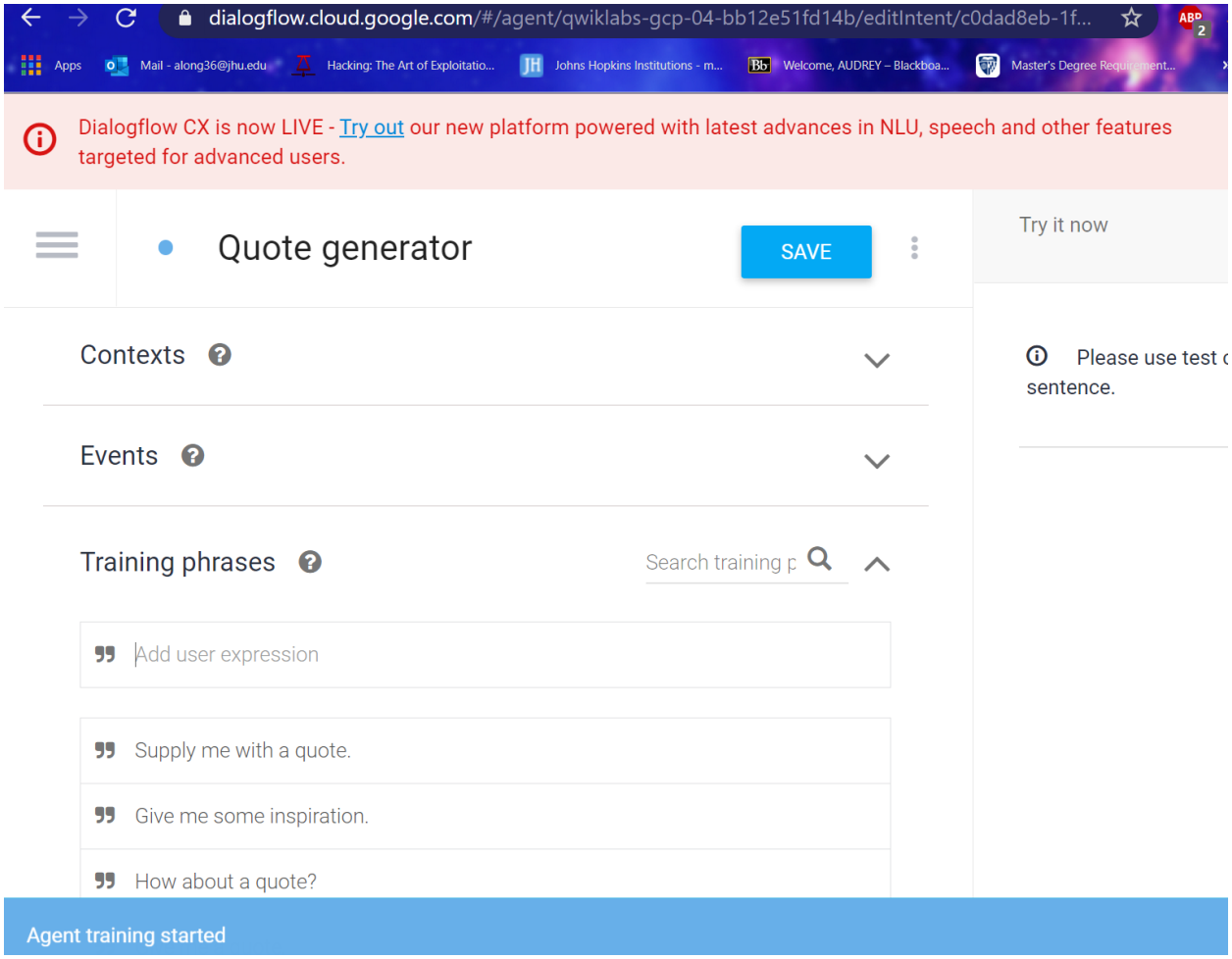


Figure 3: Build Custom Diagflow Intent

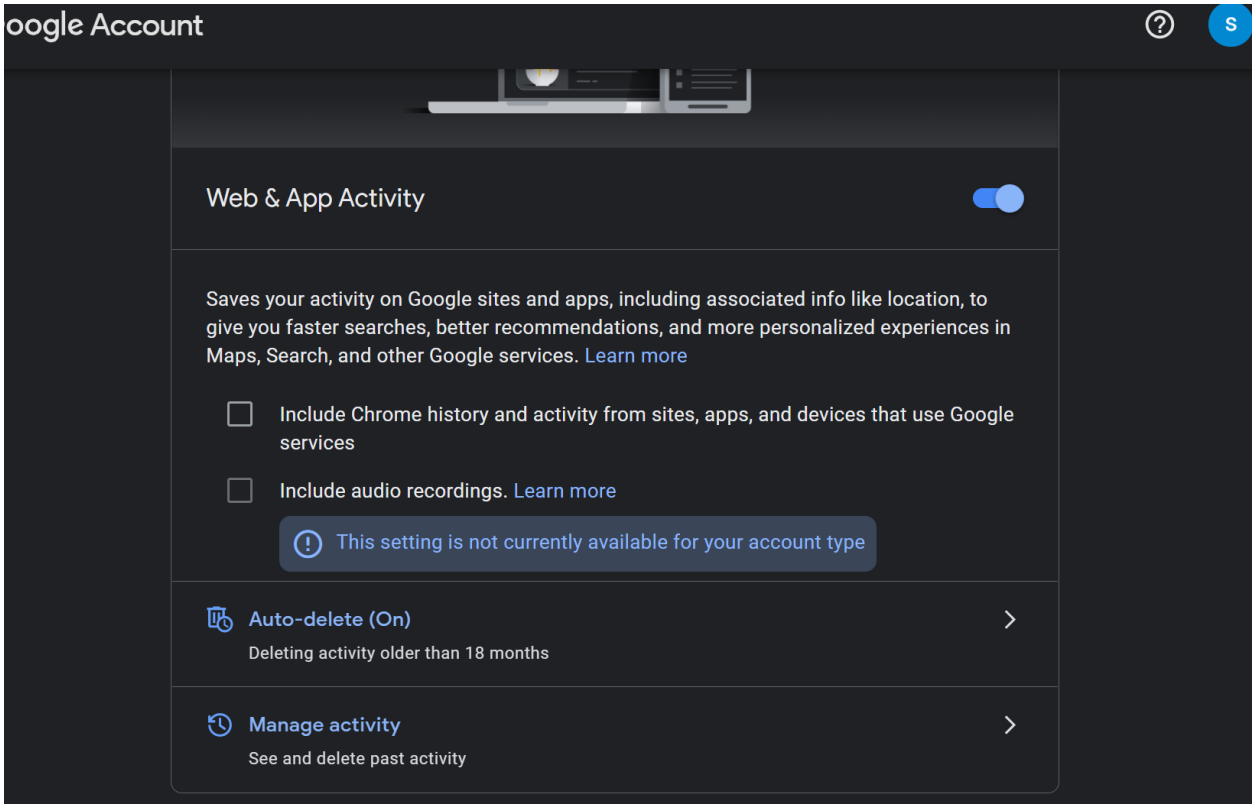


Figure 4: turn on permissions

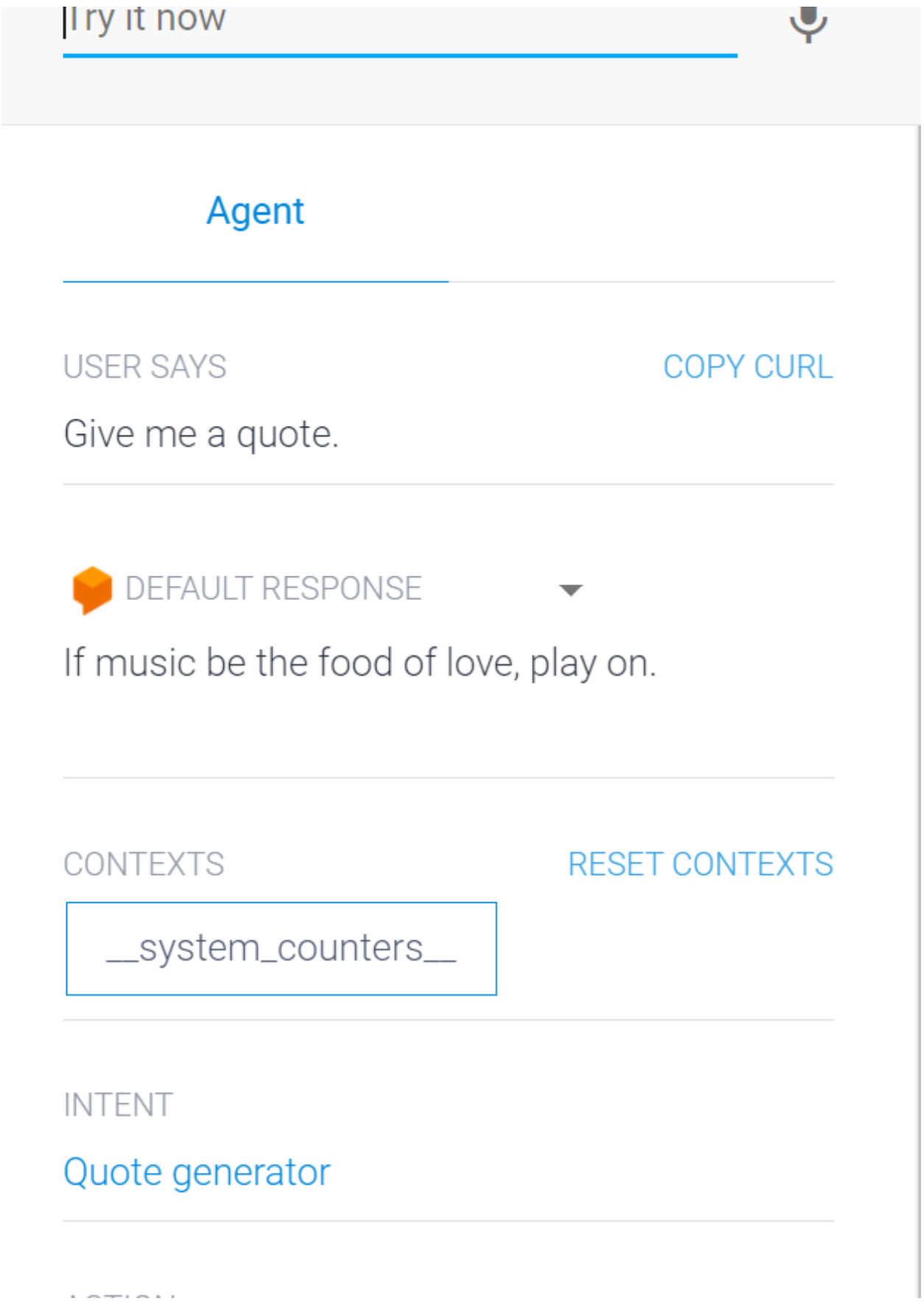

Try it now
Agent
USER SAYS
COPY CURL
Give me a quote.
DEFAULT RESPONSE
If music be the food of love, play on.
CONTEXTS
RESET CONTEXTS
__system_counters__
INTENT
Quote generator

Figure 5: test quote generator

2. How does Google handle authentication for account linking?
Oauth2 based Google sign in. Google Account Linking with OAuth bookmark_border. Accounts are linked using industry standard OAuth 2.0 implicit and authorization code flows. [7]

3. Where does Dialogflow store your data?
The userStorage field of your AppResponse object is a string that contains an opaque token supplied by the Action that is saved across conversations for a particular user. [8]

4. How does Dialogflow/Google protect your data while intransit and at rest?

Google uses several layers of encryption to protect customer data at rest in Google Cloud products. Google Cloud encrypts all customer content stored at rest, without any action required from the customer, using one or more encryption mechanisms.
[9]

5. What service should be used for monitoring and logging?

Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization:

- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs [10]

6. What are the 3 options Google offers for viewing and interacting with your logs?

1.) Legacy log viewer
2.) Big Query
3.) Cloud audit logs

Assignment Deliverables: Please submit the three Parts: A, B, C in a PDF or Word Document.

References

https://www.hindawi.com/journals/ijap/2015/630674/ [1]

http://www.elektrorevue.cz/en/download/bandwidth-efficiency-of-wireless-networks-of-wpan--wlan--wman-and-wwan-1/#:~:text=It%20guarantees%20a%20bitrate%20of,voice%2C%20data%20

and%20multimedia%20services.&text=WWAN%20provides%20for%20users%20the,remote%20public%20or%20private%20networks. [2]

https://www.sciencedirect.com/topics/computer-science/wireless-wide-area-network [3]

https://en.wikipedia.org/wiki/Wireless_WAN [4]

https://link.springer.com/chapter/10.1007%2F978-1-4020-5397-9_6 [5]

https://docs.aws.amazon.com/iot/latest/developerguide/vulnerability-analysis-and-management.html [6]

https://developers.google.com/identity/account-linking/oauth-linking [7]

https://developers.google.com/assistant/conversational/df-asdk/save-data#saving_data_between_turns_of_a_conversation [8]

https://cloud.google.com/security/encryption-at-rest/default-encryption [9]

https://cloud.google.com/dialogflow/es/docs/reference/audit-logging [10]