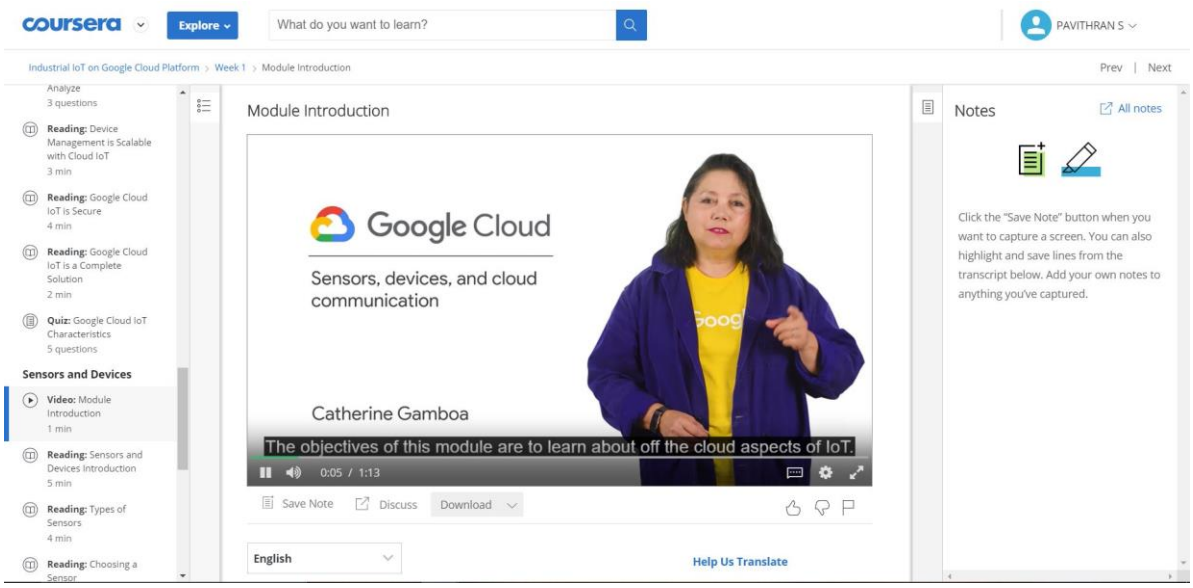
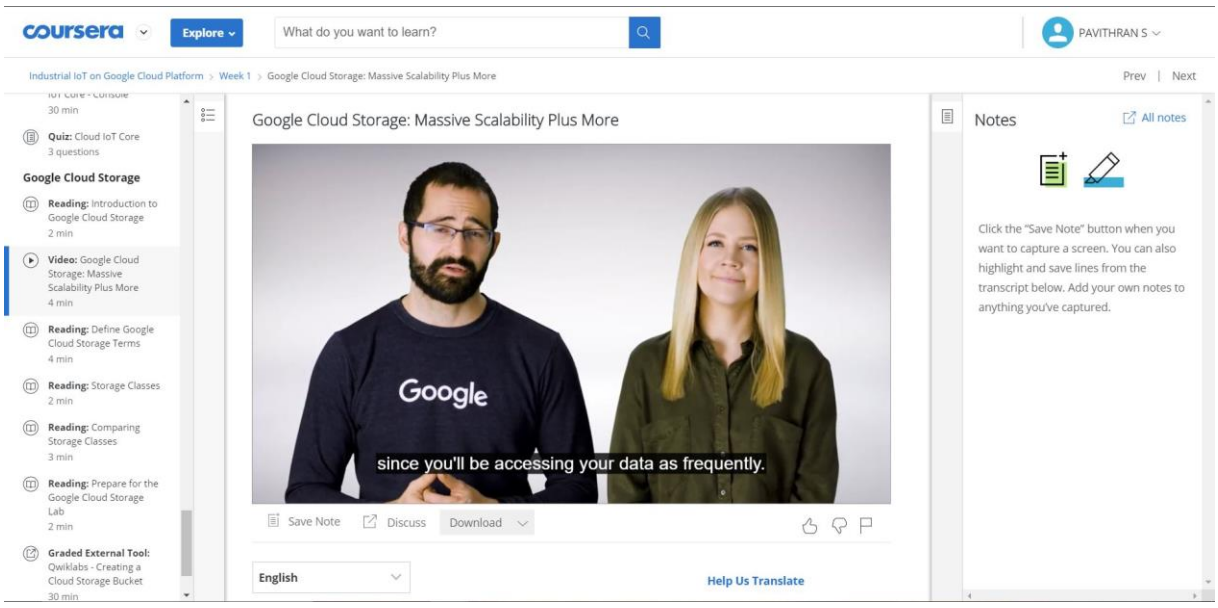
DAILY ASSESSMENT FORMAT

Date:	06 AUG 2020	Name:	PAVITHRAN S
Course:	industrial iot on google cloud platform	USN:	4AL17EC068
Topic:	industrial iot on google cloud platform	Semester & Section:	6TH B
Github Repository:	Pavithran		

FORENOON SESSION DETAILS
Image of session





Report – Report can be typed or hand written for up to two pages.

Challenges in IIoT

Choosing the right IoT platform is a complex endeavor, and it is critical for enterprise to get it right.

When designing an IoT network, you should take the following issues into consideration:

Connectivity: At present, IoT relies on a server/client model to authenticate, authorize, and connect devices to nodes in the network. Although this model works for hundreds or even thousands of devices, it will become unworkable as numbers grow to the millions and billions per network. Without proper throughput design considerations, bottlenecks may occur during the information exchange at the server. In the future, off-loading tasks to the edge will become important. This means that IoT networks will need devices capable of handling data analysis, machine learning, and data gathering.

Brownfield deployment (legacy infrastructure): As IoT devices and networks age and new technology emerges, brownfield deployment will become an issue. Companies will need to confront the task of integrating new devices and technologies into existing networks.

Security and compliance: As you may have seen, hacking IoT devices has already occurred. Everything from baby monitors, to cars, to refrigerators has been exploited. As networks grow, without adequate security, each added node can become a potential opening for hacking.

Dealing with non-standard communication protocol: Networks will need to handle ever-increasing amounts of data from sensors. Data handling, processing, and storing will increase as data input loads increase, while at the same time, the value of data increases with the size, depth, and frequency of data available to data analytics.

IT/OT convergence: The integration of information technology and operational technology is converging with industrial applications of the Internet of Things (IIoT). IT has traditionally been data-centric, while OT has been used to monitor events. IoT has blurred this distinction as devices monitor and generate massive amounts of data. Enterprise and industrial operations will need to modify and adjust their processes to accommodate IIoT devices and data.

Get actionable intelligence from data: The value of data increases as the ability to get actionable intelligence from it increases. IoT analysis will need to be able to handle unstructured data, massive amounts of real-time data, and outliers in real time.

Device Management is Scalable with Cloud IoT

Devices in an IoT network must be securely connected to the network, new devices must be easily added, and all devices must be easily updated when necessary. IoT networks often contain hundreds, thousands, or even millions of devices.

Managing a network means managing *all the devices* in the network. With Cloud IoT you can easily and securely connect, manage, and ingest IoT data from globally dispersed devices at scale.

Cloud IoT Core is where users create registries and devices. A Pub/Sub topic is selected when a registry is created. Authorizations and keys are associated with each device as it is added to the registry.

Device management on Cloud IoT covers the three main concerns of sensor and device management: adding new devices, monitoring devices, and updating devices.

Adding new devices

Google Cloud IoT ensures:

- a device has at least an ID and basic metadata before it can connect to Google Cloud
- credentials and authentication are checked before allowing a device to connect to Google cloud.
- device is authorized to publish or subscribe to a topic on Cloud Pub/Sub.
- a secure network connection with Google Cloud.
- devices are registered and tracked when they are used. Details about the device include: Heartbeat, telemetry event received, config set, config acknowledge, and errors.

Monitoring devices

Cloud IoT Core monitors the daily operations and status of devices with Stackdriver Logging. The level of Stackdriver Logging for each device is specified when the device is created. The four levels of Stackdriver Logging are:

- None - no logging of the device is maintained by Stackdriver
- Error - record only error messages associated with the device
- Info - log errors, status, and state of the device
- Debug - record debug level information for the device

Updating devices

When working with large networks, updating devices individually is not practical, or in some cases, even

possible. Cloud IoT gives you the option to push updates over the air (OTA).