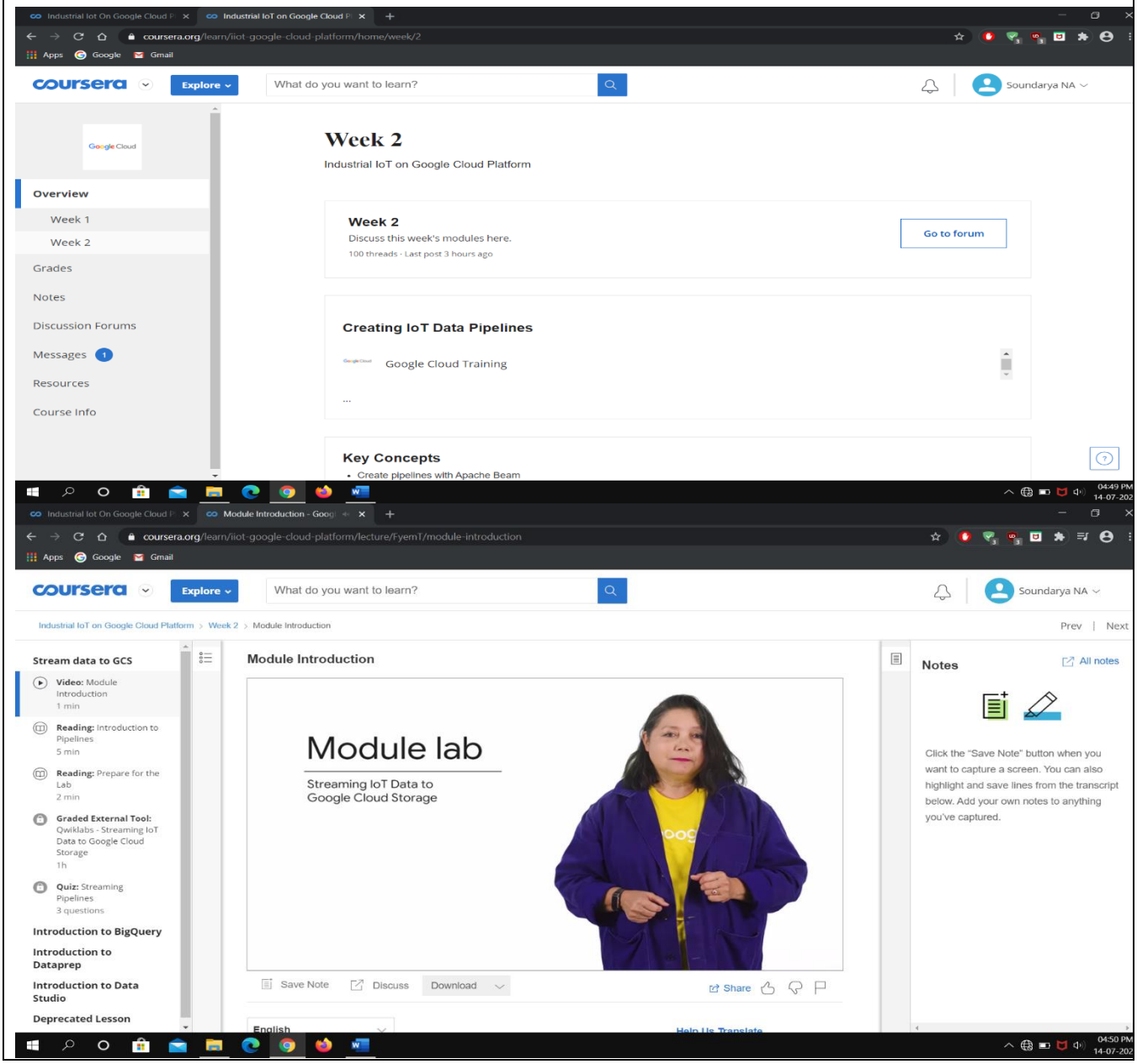
DAILY ASSESSMENT FORMAT

Date:	14th July2020	**Name:**	Soundarya NA
Course:	Coursera	**USN:**	4AL16EC077
Topic:	Industrial IOT on Google Cloud Platform	**Semester & Section:**	8th - B
Github Repository:	Soundaryana-courses		

FORENOON SESSION DETAILS

Image of session



Report:

Introduction to Pipelines:

The Internet of Things is nothing less than a revolution, disrupting businesses and changing the way we engage with our surroundings. The ability to connect everyday devices to the cloud, receive information, analyze data, gain insights and perform actions will enhance our personal comfort and convenience, create new business opportunities and reduce waste and pollution.

IoT devices can be roughly divided into three categories: sensors, connectors and smart devices. Sensors are simple, cheap devices, aimed at collecting data from the environment (for example, the lighting sensors on a street pole). They utilize short range communication protocols and are usually aggregated to a local "mesh" network with a central gateway that connects them to the cloud. These sensors allow the transformation of still objects, such as poles, highways and bridges, into "smart" objects. Connectors are simple network devices aimed at connecting not-so-smart appliances to the web. For instance, a connector could turn a regular kettle into a smart one, allowing the owner to remotely control it. Smart devices, like security cameras, routers or Amazon's Alexa, are more complex. These Linux or Android-based devices have some computation power and an IP address and are quickly gaining popularity in the commercial and consumer space.

IOT adoption:

The pace of change is astounding: 127 new devices are connected to the Internet every second according to McKinsey, and Gartner predicts that over 20.4 billion devices will be in use by 2020. This usage volume encompasses both the consumer space and the commercial space— and each vertical has its own differentiating characteristics.

Consumer IoT devices are proliferating in homes and offices with the promise of convenience and efficiency. Smart TVs, digital set-top boxes, smart speakers and personal helpers lead this charge, followed by smart fridges, security cameras and intrusion detection systems. According to recent surveys, 90 percent of U.S. consumers own a smart home device. Furthermore, over 30 percent who do not have a connected home device plan to purchase one within the year. The drivers for this rapid

adoption are the will to facilitate life and simplify domestic tasks, along with the desire to appear innovative (74 percent of respondents think connected home devices are the wave of the future).
For the commercial sector, the motivations for adopting IoT are different. This sector is comprised of multiple verticals, each with its own requirements. The main drivers for adoption in the commercial sector are cost savings, increased efficiency and improved data collection and analysis. As with the consumer sector, there are clear leaders in adoption: smart electric meters and commercial security cameras are pushing ahead, followed by industrial and transportation solutions.

In the commercial space, smart city projects—including traffic management, smart utilities, lighting, environmental monitoring and public safety and surveillance—lead the way in terms of adoption, accounting for 23 percent of all IoT projects. Next is the connected industry (sometimes referred to as Industrial IoT) and connected buildings.

Additional sectors will eventually embrace IoT. Agriculture, mining and energy are testbeds for IoT technologies but, given the traditionalist leanings within these industries, we can assume that adoption will be slower.

Of the many reasons cited for this slow adoption, the two that stand out are privacy and security risks (although they seem to be more relevant to the commercial than the consumer sector). This is not surprising; the same pushback can be seen throughout history whenever new technologies appear. But since large-scale cyberattacks utilizing IoT devices and very public privacy glitches (like those involving smart toys) are a factor, decision makers cannot be blamed for taking a more cautious approach and trying to gain a better understanding of the threat landscape before jumping on the IoT wagon.

Current threats and risks:

Current threats pertaining to IoT can be divided into two categories: threats that leverage IoT devices and direct threats to the devices themselves.

As IoT devices become more established in enterprises, factories and organizations, there's a growing fear that these devices will be leveraged to launch an attack on the organizations' networks, with the aim of stealing information or money.

The main challenge is that an IoT device could be brought into the organization and connected to local networks without the knowledge of the IT department (this is sometimes known as "Shadow IoT"), thereby creating a breach. However, this internal IoT threat can be mitigated through means similar to what organizations use today, and eventually IoT security solutions will be fully integrated into IT security departments.

The second threat is to the IoT devices themselves. These devices are deployed on the streets, in people's homes and in enterprises, often without supervision or monitoring. Being so exposed, they are vulnerable to cyberattacks. An infected IoT device can be utilized to mine cryptocurrencies, launch denial of service attacks, recruit other devices to a botnet, or even steal the video and audio information that the device is recording and interfere with its operation. When an IoT device is infected, it is overworked, leading to overall degradation in performance. This means that the device consumes excess power and bandwidth and disconnects and breaks more often, creating a substantial commercial impact on the IoT service provider.

Securing such devices is a much more complicated problem than securing enterprises from IoT threats. The complexity is because of the great diversity of IoT devices as well as their deployment in an enormous number of places. Additionally, it's not always clear who is responsible for securing them, and—to add one more layer to the equation—traditional security mechanisms are insufficient.
Let's take, for example, a smart city deployment. The municipality is the end client of the project, but the project is owned and maintained by an integrator who sells it to the municipality as a managed service. In this scenario, who is in charge of securing the device? And who should bear the cost? Moving beyond the responsibility question, providing security for devices by adopting traditional security mechanisms isn't practical. It would require deploying multiple firewalls and network monitoring equipment, which is much more expensive than the IoT devices themselves.

Mitigation:

The mitigation of IoT threats must happen on several levels. On the device itself, information must be collected to allow real-time monitoring. In some cases, automatic mitigation—wherein the device is blocked from searching for other devices and trying to infect them—needs to be put into place as well. An additional layer of security should reside in the cloud, with big data analytics and machine learning algorithms looking for anomalies that indicate infection, account hijacks and malicious use by insiders. A centralized security operations center should be put in place to monitor all these activities and intervene in the case of a severe alert. This is crucial because most companies today don't have the necessary manpower to manage their cybersecurity operations, and it is highly unlikely that they will be able to manage the IoT security side with such limited personnel. Moreover, IoT security is novel and unique and requires a skill set that touches upon hardware, software, cloud and analytics—a comprehensive expertise which can be very hard to find in one security person. Just as with IT security, the option of using an outsourced, managed security service is probably preferable for most companies and IoT service providers.