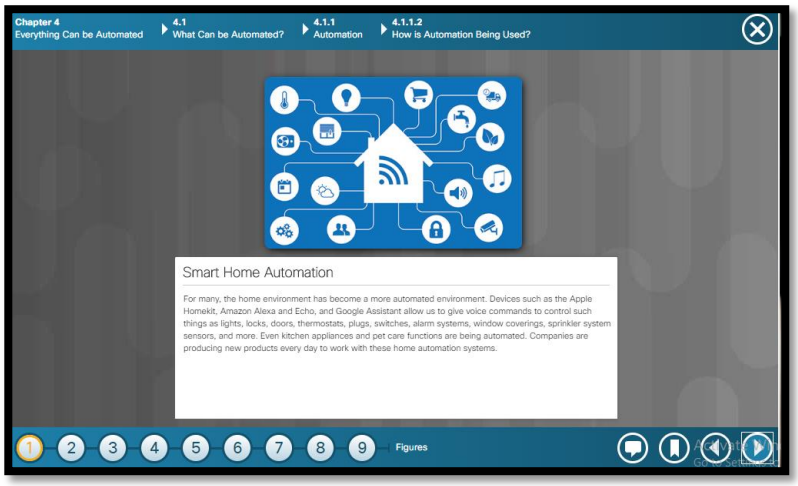
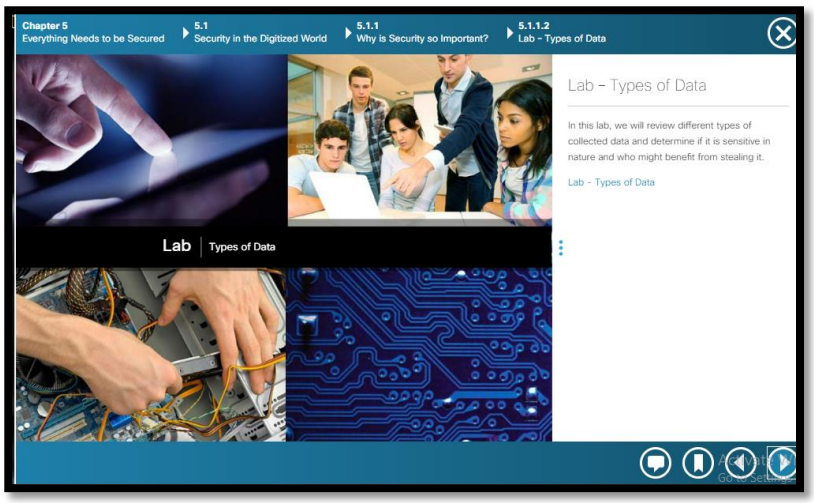
DAILY ASSESSMENT

Date:	**09/07/2020**	**Name:**	**Davis S. Patel**
Course:	**Cisco - IOT**	**USN:**	**4AL16EC045**
Topic:	**Everything can be Automated Everything Needs to be Secured**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

FORENOON SESSION DETAILS
Image of session





This quiz covers the content presented in **I2IoT 2.0 Chapter 4**. This quiz is designed for practice. You will be allowed multiple attempts and the grade does not appear in the gradebook.

There are multiple task types that may be available in this quiz. In some task types, partial credit scoring is allowed to foster learning. Please note that on tasks with multiple answers, points can be deducted for selecting incorrect options.

At the completion of the quiz, some items may display feedback. The feedback will reference the source of the content. Example: "Refer to curriculum topic: 1.2.3" - indicates that the source of the material for this task is located in chapter 1, section 2, topic 3.

Form: 35282

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	4 minutes	25 out of 30

This quiz covers the content presented in **I2IoT 2.0 Chapter 5**. This quiz is designed for practice. You will be allowed multiple attempts and the grade does not appear in the gradebook.

There are multiple task types that may be available in this quiz. In some task types, partial credit scoring is allowed to foster learning. Please note that on tasks with multiple answers, points can be deducted for selecting incorrect options.

At the completion of the quiz, some items may display feedback. The feedback will reference the source of the content. Example: "Refer to curriculum topic: 1.2.3" - indicates that the source of the material for this task is located in chapter 1, section 2, topic 3.

Form: 35283

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	5 minutes	30 out of 30

REPORT –

Automation is any process that is self-driven and reduces, then eventually eliminates, the need for human intervention.

Automation was once confined to the manufacturing industry. Highly repetitive tasks such as automobile assembly were turned over to machines and the modern assembly line was born. Machines are excellent at repeating the same task without fatigue and without the errors that humans are prone to make in such jobs. This results in greater output, because machines can work 24 hours a day without breaks. Machines also provide a more uniform product.

The IoT opens up a new world in which tasks previously requiring human intervention can become automated. As we have seen, the IoT allows the collection of vast amounts of data that can be quickly analyzed to provide information that can help guide an event or process.

As we continue to embrace the benefits of the IoT, automation becomes increasingly important. Access to huge amounts of quickly processed sensor data started people thinking about how to apply the concepts of machine learning and automation to everyday tasks. Many routine tasks are being automated to improve their accuracy and efficiency.

Automation is often tied to the field of robotics. Robots are used in dangerous conditions such as mining, firefighting, and cleaning up industrial accidents, reducing the risk to humans. They are also used in such tasks as automated assembly lines.

We now see automation everywhere, from self-serve checkouts at stores and automatic building environmental controls, to autonomous cars and planes.

ML in the IoT

One of the features of the IoT is that it enables the collection of extremely large pools of data that can "teach" programs how to respond in certain conditions. Some of the more common uses of ML technology include:

- **Speech Recognition** - Many different companies now offer digital assistants which allow you to use speech to communicate with a computer system. Apple, Microsoft, Google and Amazon all offer this service. These companies not only allow commands to be given verbally, but offer speech-to-text capabilities.

- **Product Recommendation** - Systems build up a customer profile and recommend products or services based on previous patterns. Users of Amazon and eBay receive recommendations on products. Organizations such as LinkedIn, Facebook, and GooglePlus recommend users you may wish to connect with.
- **Shape Recognition** - Programs exist that allow crude hand-drawn diagrams and notes to be converted to more formal diagrams and text. This allows the shapes and lines of hand writing to be converted to more formal text which can then be searched and analyzed.
- **Credit Card Fraud Detection** - A profile is constructed about the purchasing patterns of a client. Any deviation from these patterns triggers an alert and the system automatically takes action. This action ranges from denying the transaction to notifying the authorities. Some of the events that are detected and could indicate a fraudulent transaction include purchasing products not normally purchased, purchases in a different geographic area, rapidly purchasing many different products, and purchasing large-ticket items.
- **Facial Recognition** - Security cameras are everywhere, from stores and streets to airports and transportation hubs. These cameras continually scan the crowds, normally watching for dangerous or illegal activities, but they can also be used to identify and track individuals. The system builds a pattern of specific facial features and then watches for a match to these facial patterns triggering some action.

How are ML, AI, and IBN Linked?

Intent-based networking harnesses the power of automation, AI, and ML to control the function of a network to accomplish a specific purpose, or intent.

Intent-based networking allows the IT team to specify, in plain language, exactly what they want the network to accomplish and the network makes it happen. The network is able to translate the intent into policies and then use automation to deploy the appropriate configurations required across the network.

The intent-based network uses AI and ML to ensure that any services that are deployed meet the required service level. If they do not meet the service level, the intent-based network can

make alerts and provide suggestions for improvement. In some cases, the intent-based network can automatically reconfigure the network to comply with the service levels.

The intent-based networking model shown in the figure consists of three key elements:

- **Assurance** - The assurance element is end-to-end verification of network-wide behavior. It predicts the results of any changes, tracks compliance with the original intent, and makes recommendations or adjustments when there is a misalignment between the intent and the outcome. This stage relies heavily on AI and ML. Systems are part of a closed-loop that continually monitors performance and security of the network, and reconfigures the network to ensure compliance.
- **Translation** - The translation element is the ability to apply business intent to network configuration. The intent is what you wish to accomplish, not how it is accomplished. This intent is specified in plain language and used by the system to create policies across the system. For example, an intent might be to segment guest traffic from corporate traffic, or to enable access for remote users.
- **Activation** - The activation element occurs after the intent has been specified and the policies created. This is when individual devices are provisioned to match the intent-based policies. This can be an automated or semi-automated mode that allows the network team to verify configuration before the devices are deployed.

An intent-based network creates an agile, responsive network that scales easily and adapts to meet business requirements. It makes efficient use of highly-skilled resources and allows man and machine to work together to optimize the customer experience. Additionally, intent-based networking provides a more secure digital experience by automating time consuming or complicated processes. This makes deploying security policies much easier.

Types of Data

Has data really changed? Well technically no, data generated by computers and digital devices is still groups of 1s and 0s. That has not changed. What has changed is the quantity, volume, variety, and immediacy of the generated data.

Historically companies would have access to our information gathered from forms, spreadsheets, applications, credit card purchases and other types of files. Much of the information was stored and analyzed at a later date. Sensitive data was still collected, stored and analyzed but, historically, hackers were more interested in hacking into systems to obtain corporate or government secrets.

Today, gathered data is taking on new characteristics. The digitized world has opened the floodgates for data gathering. IoT sensor-enabled devices are collecting more and more data of a personal nature. Wearable fitness trackers, home monitoring systems, security cameras, and debit card transactions are all collecting personal data as well as business and environmental data. Data is often combined from different sources and users may be unaware of this. Combining fitness monitoring data with house monitoring data could produce data points to help map the movements or location of a homeowner. This changing type of data collection and aggregation can be used for good purposes to help the environment. It also increases the possibility of invasion of our privacy, identity theft, and corporate espionage.

Personally identifiable information (PII) or sensitive personal information (SPI) is any data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual. The data gathered by companies and government institutions can also contain sensitive information concerning corporate secrets, new product patents, or national security.

Because we are gathering and storing exponential quantities of both sensitive and informational data, it has increased the need for extra security to protect this information from natural disasters, hackers, and misuse.

Security Best Practices

Securing the network involves all of the protocols, technologies, devices, tools, and techniques that secure data and mitigate threats. Network security is largely driven by the effort to stay one step ahead of ill-intentioned hackers. Just as medical doctors attempt to prevent new illnesses while treating existing problems, network security professionals attempt to prevent potential attacks while minimizing the effects of real-time attacks.

Networks are routinely under attack. It is common to read in the news about yet another network that has been compromised. Security policies, procedures, and standards must be followed in the design of all aspects of the entire network. This should include the cables, data in transit, stored data, networking devices, and end devices.

Physical Security

Today's data centers store vast quantities of sensitive, business-critical information; therefore, physical security is an operational priority. Physical security not only protects access to the premises, but also protects people and equipment. For example, fire alarms, sprinklers, seismically-braced server racks, and redundant heating, ventilation, and air conditioning (HVAC) and UPS systems are in place to protect people and equipment.

Figure one shows a representation of a data center. Select each circle for more information.

Physical security within the data center can be divided into two areas, outside and inside.

- **Outside perimeter security** - This can include on premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - This can include continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.

Security traps provide access to the data halls where data center data is stored. As shown in Figure 2, security traps are similar to an air lock. A person must first enter the security trap using their badge ID proximity card. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. The user must repeat the process to exit the data hall.

Challenges of Securing IoT devices

IoT devices are developed with the necessary network connectivity capabilities but often do not implement strong network security. Network security is a critical factor when deploying IoT devices. Methods must be taken to ensure the authenticity, integrity, and security of the data, the path from the sensor to the collector, and the connectivity to the device.