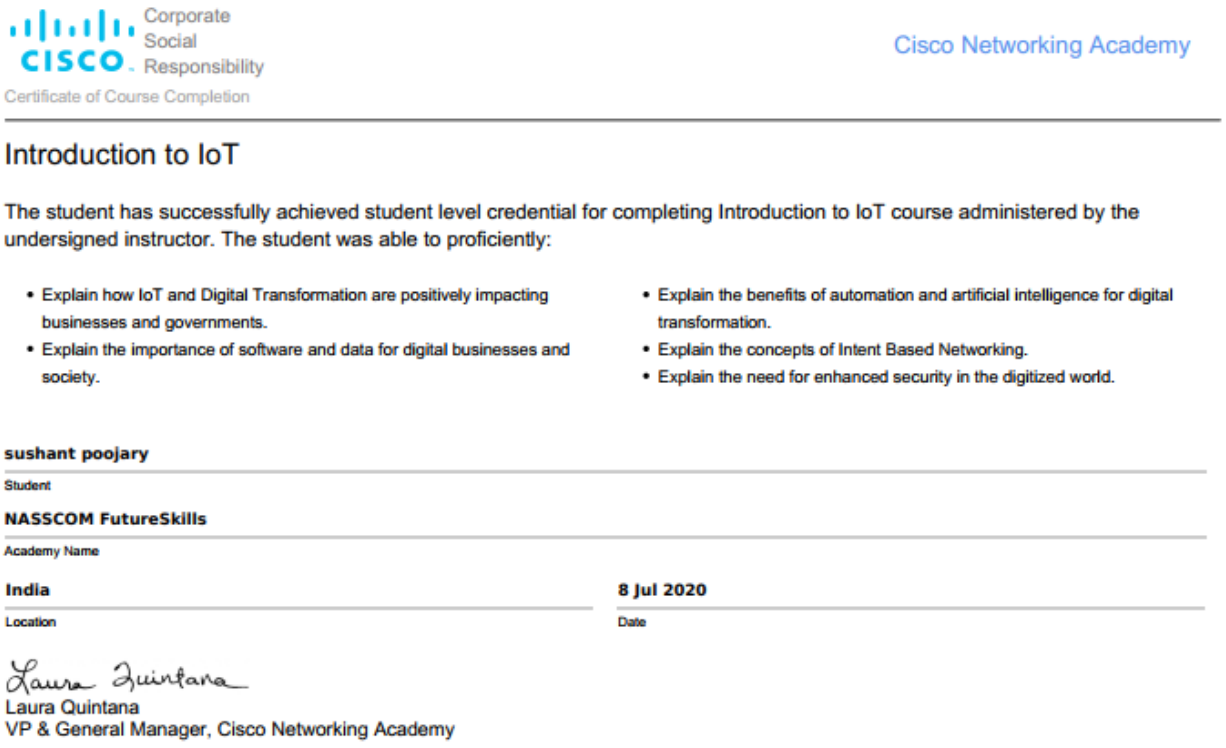
DAILY ASSESSMENT FORMAT

Date:	**10th July 2020**	**Name:**	**Poojary Sushant**
Course:	**Introduction to the Internet of Things**	**USN:**	**4AL18EC400**
Topic:	**Chapter 5: Everything Needs to be Secured** **Chapter 6:Educational and Business Opportunities**	**Semester & Section:**	**6th sem 'B"**
Github Repository:	**Sushant7026**		

FORENOON SESSION DETAILS

Image of session



Corporate Social Responsibility

Cisco Networking Academy

Certificate of Course Completion

Introduction to IoT

The student has successfully achieved student level credential for completing Introduction to IoT course administered by the undersigned instructor. The student was able to proficiently:

- Explain how IoT and Digital Transformation are positively impacting businesses and governments.
- Explain the importance of software and data for digital businesses and society.
- Explain the benefits of automation and artificial intelligence for digital transformation.
- Explain the concepts of Intent Based Networking.
- Explain the need for enhanced security in the digitized world.

sushant poojary

Student

NASSCOM FutureSkills

Academy Name

India

Location

8 Jul 2020

Date

Laura Quintana

Laura Quintana
VP & General Manager, Cisco Networking Academy

Report –

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.

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.

Smart Homes

Smart home technology has become very popular and its popularity is increasing every year as the technology evolves. Who doesn't find it appealing to turn your home thermostat up or down while you are at work, or to have your refrigerator order groceries to be delivered when you get home? How cool is it to check on the dog or to verify that your teenagers are doing their homework after school by activating your home security cameras?

As we install more and more smart sensors into our homes, we do increase the potential for security issues. Often the sensors are connected to the same network as our home or small business devices so that a breach of one device can radiate outwards to affect all connected devices. The sensors could also provide a way for hackers to get into our home network and gain access to any PCs and data that are connected to it.

Even virtual assistants such as Apple SIRI, Amazon Echo, or Google Home can be security risks. People use these devices to turn on music, adjust room temperatures, order products on-line, and get directions for where they are going. Can this cause any harm? It is possible that personal information such as passwords or credit card information could be leaked.

Fortunately many of the security flaws of the early smart technology sensors have already been discovered. Developers are working to correct the flaws and improve security measures to protect their systems from attack. Before purchasing home security systems, it is very important to research the developer and the security and encryption protocols that are in place for its products.

Challenges in the Digitized World

The IoT provides many benefits but at the same time it presents many challenges. Since the IoT is a transformational technology, we are now faced with an ever expanding collection of new technology that we must master. The IoT is changing every aspect of our lives.

This is not the first time we have experienced a technological development that has such an impact. Mechanization on the farm allowed increased productivity of available farmland and started the migration of the population from rural to urban areas. The development of the automobile allowed for greater mobility of the workforce and increased recreational activities. The personal computer allowed the automation of many routine tasks with improved accuracy and efficiency. The Internet started to break down geographic barriers and improve equality between people on a global scale. These are only a few of the transformational technologies that we have experienced in recent history.

Every one of these technologies presented major changes to an established society and was met with initial fear and apprehension. After the initial fear of the unknown was overcome and the technology was embraced, the inherent benefits became obvious. Each perceived challenge opens up many new opportunities.

Networking Academy Curriculum

The Networking Academy delivers a comprehensive, 21st century learning experience. Students develop the foundational IT skills needed to design, build, and manage networks, along with career skills such as problem solving, collaboration, and critical thinking. Students complete hands-on learning activities and network simulations to develop practical skills that will help them find their place among networking professionals around the world. These are some of the offerings of the Networking Academy:

- **IoT Fundamentals** – This series of courses teaches you about the IoT and how it can be used to enhance society. This series continues to evolve. It currently includes courses and activities to develop your skills for securely collecting data and connecting sensors to the cloud, analyzing big data, and creating your own IoT solution.

- **IT Essentials** - IT Essentials covers the fundamentals of computer hardware and software. It also introduces more advanced concepts, such as security, networking, and the responsibilities of an IT professional.

- **Entrepreneurship** - The Entrepreneurship course teaches critical business skills, financial skills, attitudes, and behaviors to help students develop an entrepreneurial mindset which can empower them to improve their overall quality of life.

- **Introduction to Cybersecurity** - The Introduction to Cybersecurity course covers trends in cybersecurity and demonstrates the need for cybersecurity skills in various industries.

- **CCNA Routing and Switching** – Cisco Certified Networking Associate (CCNA) Routing and Switching provides a comprehensive overview of networking concepts and skills. It covers skills and knowledge required for administrators of devices in small to medium-sized networks. This

curriculum has an emphasis on practical work-force readiness, and soft-skills development.

- **CCNA Security** - CCNA Security introduces the core security concepts and skills needed to install, troubleshoot, and monitor a network to maintain the integrity, confidentiality, and availability of data and devices.

- **CCNP –** The Cisco Certified Networking Professional (CCNP) curriculum is the next step for people who have completed the CCNA Routing and Switching courses.

Communities of Interest

A community of interest is a group of people who share a common interest or passion about a specific topic. These people get together to share information and ideas about this topic.

This shared interest allows the group to develop into a true community. Members of these communities are extremely knowledgeable and passionate about the topic being discussed and are willing to share their knowledge with other community members. This makes the community an excellent resource for the development of the area of interest.

The Internet allows these communities to exist virtually and span several geographic areas and time zones. Members can share files and technology in real time.