DAILY ASSESSMENT FORMAT

Date:	**09/07/2020**	**Name:**	**Nichenametla Bhargavi**
Course:	Introduction to Internet of Things	**USN:**	**4AL17EC061**
Topic:	Chapter 5	**Semester & Section:**	**6th Sem A sec**
Github	Bhargavi_Nichenametla		

AFTERNOON SESSION DETAILS

Image of the session

Report- Report can be handwritten or typed within one or two pages.

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.

Public Hotspots:

When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. Common activities on public Wi-Fi include logging into a personal email account, entering personally identifiable information, logging into social media, and accessing bank or financial information. All of this information could be stolen if the Wi-Fi connection is unsecure.

Safety rules to follow if you are using a public or unsecure Wi-Fi hotspot:

* Do not access or send any sensitive personal information over a public wireless network.

* Verify whether your computer is configured with file and media sharing, and that it requires user authentication with encryption.

Use encrypted virtual private network (VPN) tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

Many mobile devices, such as smartphones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off when you are not using it.

Setting Up a VPN on Smartphones:

A VPN is a secure network using an encrypted Internet connection that acts as a secure "tunnel" for data. It can be created over the public Internet connection to enable users to hide their identity when they are using the Internet. You should use a VPN service when you connect to a Wi-Fi network that is not your own (e.g. at the library or coffee shop). It prevents others on that public network from eavesdropping on your web use when you are using non-secure websites or communications.

Many businesses require VPN access into their internal networks if employees are working remotely or are mobile. The employee will be provided with the VPN client, as well as user ID and password information. For those who do not have access to a business VPN, there are many smartphone VPN service applications that you can download for free or for a monthly fee. Examples of these VPN apps include: ExpressVPN, NordVPN, and TunnelBear.

Summary:

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. Legitimate companies have an agreements (Terms and Conditions or Terms of Service) that gives them permission to use the collected data about you for purposes of improving their business. Other legitimate users of our data would be companies that use sensors on their own devices or vehicles. Governments that have environmental sensors, and cities who have installed sensors on trains, busses or traffic lights also have a right to the data they generate.

Some hackers, called white hat hackers, are paid by legitimate companies and governments to test the security of a device or system. Their goal is not to steal or modify data but to help to protect it. Black hat hackers want access to collected data for many reasons, including selling it, damaging the reputation of a person or company, and causing political unrest.