**DAILY ASSESSMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **09/07/2020** | **Name:** | **Dhavala** |
| **Course:** | **Introduction to internet of things** | **USN:** | **4AL17EC027** |
| **Topic:** | * **Everything needs to be secured** | **Semester & Section:** | **6TH SEM & A Section** |
| **Github Repository:** | **Dhavala27** |  |  |

|  |
| --- |
| **SESSION DETAILS**      **Types of 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.  **Internet fingerprint**  The purpose of this lab is to introduce the aspect of “fingerprinting” an individual using the worldwide web. The objective is to introduce various methods to extract as much information as possible using only the Internet browser and various sites effectively.  **Setting up of VPN on smart phone**  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](https://www.expressvpn.com/" \t "_blank), [NordVPN](https://nordvpn.com/" \t "_blank), and [TunnelBear](https://www.tunnelbear.com/" \t "_blank).  If you have a business VPN or if you download a VPN service application, they will provide the information and support required to set up your VPN. Select Figure 1 for instructions to manually set up a VPN on an Android device. Select Figure 2 for instructions to manually set up a VPN on an iPhone or iPad.  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.  Next, the chapter detailed security best practices. Security includes physically securing the outside and inside perimeters of places, such as data centers, where data is stored. Securing IoT devices is challenging due to the sheer number of them, the fact that they are found in non-traditional locations, and that many of them cannot be upgraded.  Black hat hackers frequently access available Wi-Fi. There are many steps you can take to protect your company’s wireless network. To protect devices, keeps the firewall turned on, manage your operating system and browser, and use antivirus and antispyware.  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.   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. |