**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **09/07/2020** | **Name:** | **Namratha S Hipparagi** |
| **Course:** | **Cisco** | **USN:** | **4AL16EC040** |
| **Topic:** | **Everything needs to be secured** | **Semester & Section:** | **8th A** |
| **Github Repository:** | **namrathahipparagi\_1** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **FORENOON SESSION DETAILS** | | | | | |
| **Image of session** | | | | | |
| **REPORT** **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. 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. 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. 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. 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.  **The Good Guys**  Legitimate companies have an agreement in place that gives them permission to use the collected data about you for purposes of improving their business. 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. Remember those “Terms and Conditions” or “Terms of Service and Agreements” documents that we say yes to but do not usually read? The next time that you are presented with one, take the time to read through it. The contents might surprise you.  **The Bad Guys**  Other hackers, called black hat hackers, want access to collected data for many nefarious reasons:   * To sell the information to a third party. * To access data to commit a crime. * To hack into systems to prove that they can do it. * To modify the data or disable functionality on a device. * To disrupt or to damage the image of a legitimate company. | | | | | |
| **Date:** | **09/07/2020** | **Name:** | **Namratha S Hipparagi** |
| **Course:** | **Coursera – AI** | **USN:** | **4AL16EC040** |
| **Topic:** | **Introduction** | **Semester & Section:** | **8th A** |

|  |
| --- |
| **AFTERNOON SESSION DETAILS** |
| **REPORT**  **Machine learning** (**ML**) is the study of computer algorithms that improve automatically through experience. It is seen as a subset of [artificial intelligence](https://en.wikipedia.org/wiki/Artificial_intelligence). Machine learning algorithms build a [mathematical model](https://en.wikipedia.org/wiki/Mathematical_model) based on sample data, known as "[training data](https://en.wikipedia.org/wiki/Training_data)", in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of applications, such as [email filtering](https://en.wikipedia.org/wiki/Email_filtering) and [computer vision](https://en.wikipedia.org/wiki/Computer_vision), where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks. **Machine learning approaches** Machine learning approaches are traditionally divided into three broad categories, depending on the nature of the "signal" or "feedback" available to the learning system:   * [Supervised learning](https://en.wikipedia.org/wiki/Supervised_learning): The computer is presented with example inputs and their desired outputs, given by a "teacher", and the goal is to learn a general rule that [maps](https://en.wikipedia.org/wiki/Map_(mathematics)) inputs to outputs. * [Unsupervised learning](https://en.wikipedia.org/wiki/Unsupervised_learning): No labels are given to the learning algorithm, leaving it on its own to find structure in its input. Unsupervised learning can be a goal in itself (discovering hidden patterns in data) or a means towards an end ([feature learning](https://en.wikipedia.org/wiki/Feature_learning)). * [Reinforcement learning](https://en.wikipedia.org/wiki/Reinforcement_learning): A computer program interacts with a dynamic environment in which it must perform a certain goal (such as [driving a vehicle](https://en.wikipedia.org/wiki/Autonomous_car) or playing a game against an opponent). As it navigates its problem space, the program is provided feedback that's analogous to rewards, which it tries to maximise.     Each training example has one or more inputs and the desired output, also known as a supervisory signal. In the mathematical model, each training example is represented by an [array](https://en.wikipedia.org/wiki/Array_data_structure) or vector, sometimes called a feature vector, and the training data is represented by a [matrix](https://en.wikipedia.org/wiki/Matrix_(mathematics)). Through iterative optimization of an [objective function](https://en.wikipedia.org/wiki/Loss_function), supervised learning algorithms learn a function that can be used to predict the output associated with new inputs. An optimal function will allow the algorithm to correctly determine the output for inputs that were not a part of the training data. An algorithm that improves the accuracy of its outputs or predictions over time is said to have learned to perform that task. [Similarity learning](https://en.wikipedia.org/wiki/Similarity_learning) is an area of supervised machine learning closely related to regression and classification, but the goal is to learn from examples using a similarity function that measures how similar or related two objects are. It has applications in [ranking](https://en.wikipedia.org/wiki/Ranking), [recommendation systems](https://en.wikipedia.org/wiki/Recommendation_systems), visual identity tracking, face verification, and speaker verification. |