

29. Aprendizaje automático

Sunday, August 30, 2020 6:45 PM

El aprendizaje automático es una técnica que permite entrenar los sistemas para reconocer patrones sin describirlos explícitamente, es considerada una rama de la inteligencia artificial. La base del aprendizaje automático es la creación y entrenamiento de un modelo, un sistema que se prepara con datos de entrenamiento y luego puede procesar automáticamente nuevos datos que son similares a los datos de entrenamiento.

El modelo aprende de los datos de entrenamiento. Por ejemplo, un método tradicional para detectar spam en correos electrónicos consiste en comprobar palabras u oraciones sospechosas. En cambio, con las técnicas de aprendizaje automático, se proporciona al modelo una lista de mensajes de spam y no spam, y el sistema se ajusta por sí mismo. Aprende de los datos. Luego, se pueden entregar nuevos correos electrónicos al modelo para detectar si son spam o no.

Este enfoque también se puede usar con imágenes, por lo que en lugar de intentar crear un algoritmo de detección de formas complicado para reconocer a un perro, se puede usar una cantidad significativa de imágenes de perros para entrenar al modelo para que detecte si hay un perro o no en una imagen. El mismo enfoque se puede utilizar para otras áreas, como el sonido (voz a texto y texto a voz) y video. Este tipo de formación se denomina "supervisada" porque los datos de formación deben etiquetarse correctamente de antemano.

Este es el tipo de aprendizaje automático más maduro y útil en este momento. Hay otros tipos de aprendizaje automático que funcionan sin supervisión (donde los datos de entrenamiento no necesitan etiquetas), por ejemplo, determinando a partir de un grupo de imágenes cuáles están relacionadas entre sí.

El aprendizaje automático se está volviendo cada vez más popular. A medida que pasa el tiempo, los modelos de aprendizaje automático se vuelven más capaces y producen mejores resultados. Este solía ser un campo complicado de ingresar, pero gracias a los nuevos proveedores de la nube, las API's listas para usar están disponibles para aprovechar el poder del aprendizaje automático rápidamente.

Usos de aprendizaje automático en Ciberseguridad

- Detección de intrusos.
- Análisis de amenazas con TPV (Terminales de Punto de Venta) móviles
- Acabar con amenazas de tipo día cero

Referencias

- <https://machinelearningmastery.com/machine-learning-in-python-step-by-step/>
- Podcast: Mercedes Benz Machine Learning Research - <https://podcasts.google.com/?feed=aHR0cHM6Ly9kYXRhc2tldHRpYy5saWJzeW4uY29tL3Jzcw&ep=14&episode=Y2U2NGNkZGY2NDg3MTY5MzNIODk2ZDEwZDlmZTk0NWwM>
- Aplicaciones de ML, Dr. León Palafox, UNAM, Banorte - <https://youtu.be/l4u4nxEO9yw>

