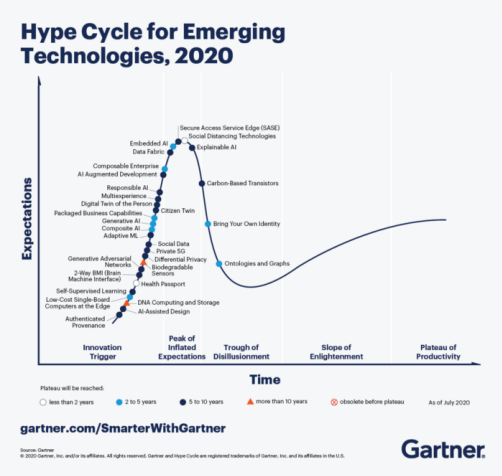
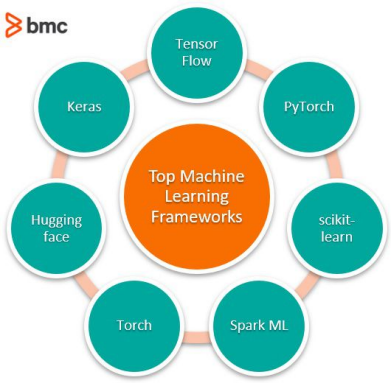
Arreglos, experiencia y conclusiones.

Teniendo en cuenta que este es el quinto y último post para la asignatura de auditoría me gustaría aprovecharlo para hablar de ciertos temas que hubiera sido lo correcto ahondar en ellos durante el segundo post y finalmente me gustaría aportar mi experiencia trabajando con ML y como yo mismo aplique los controles mencionados en el post anterior.



Me parece interesante mirar a los gráficos que hace Gartner, una de las consultoras más importantes que existen, sobre las tendencias más actuales y muestra su estado en lo que se conoce como ciclo de la expectación (hype cycle) en el de este año 2020 en lo que a IA/ML se refiere, nos encontramos temas bastante innovadores como la IA responsible, la IA embebida o incluso la IA explicable lo cual nos dice que en esta materia se siguen haciendo avances. Y si miramos 5 años atrás nos encontramos con que el machine learning se encontraba en ese pico de expectación y no desaparecería de ahí hasta el año 2018 para ser sustituida por un campo de gran complejidad en el campo del machine learning como lo son las redes neuronales profundas [1]. Todo esto nos dice que son tecnologías sobre las que se ha investigado de forma muy profunda y que ya tienen cierto recorrido.

Ahora mismo, y como se vio en el primer post que hice para esta asignatura, existen infinidad de algoritmos y métodos para desarrollar una herramienta que hagan uso de estos sistemas, lo mejor de todo, es que simultáneamente existen multitud de herramientas para construir este tipo de sistemas (ya sean ML o incluso para trabajar con redes neuronales) como scikt-learn, pyTorch o Tensorflow.



Buscando información sobre la existencia de estándares en la inteligencia artificial, me he encontrado con el ISO/IEC JTC 1/SC 42 que detalla referencias, guías, procesos, etc. sobre cómo trabajar con esta tecnología. El problema que veo aquí es que a diferencia de otras tecnologías recientes como el IoT solamente tiene seis estándares publicados y otros veintiuno están en proceso de aprobación [2]. Al ser una tecnología relativamente reciente no existen tantos estándares sobre los que una empresa pueda apoyarse.

En cuanto a los casos de uso que puede tener esta tecnología, creo que casi a diario podemos verlos y no nos damos cuenta hasta que nos lo dicen a la cara. Por ejemplo, la red social Twitter usa el machine learning con el objetivo de mostrar contenido que le guste a los usuarios para poder mantenerlos de forma activa consumiendo contenido [3]. Lo mismo ocurre con plataformas como Youtube, que aprenden de nosotros mismos con el contenido que nosotros consumimos y tanto los gigantes digitales, como las empresas tradicionales están empezando a hacer uso de los datos que nosotros generamos para poder hacer decisiones efectivas. Además de estos casos de uso centrados en los datos que generamos nosotros como usuarios también

existe el, algo desaparecido, coche autónomo que está comenzando a bajar en la gráfica de la expectación de gartner y que por lo que se va escuchando poco a poco se empieza a consolidar.

Para terminar con los arreglos al segundo post, me gustaría hablar sobre el framework CRISP-DM para auditar machine learning. A modo de resumen, en este modelo se determinan ciertos pasos a tomar para auditar estos sistemas. El primer paso es obtener conocimiento sobre el negocio en el que se va a aplicar, después se deben entender los datos y el significado que tienen estos, lo siguiente sería recoger y preparar estos datos para poder realizar un modelo y evaluarlo, una vez esto último es satisfactorio, finalmente se puede desplegar un sistema ML. Este framework está pensado para realizar una auditoría a alto nivel del machine learning y que si se requiere profundizar, se requieren expertos en la materia [4].

Antes de terminar dando mis conclusiones en el post, me gustaría hablar un poco de mi experiencia trabajando con este campo en concreto, realicé mi TFG sobre deep learning aplicado a la detección de anomalías, y cuando en los posts sobre los riesgos parece que me quedé corto y quizás algo superficial con los riesgos, creo que hice mención de los más importantes y que yo mismo tuve que hacer frente usando los controles mencionados en el post anterior a este. Creo que solucionando esos riesgos se puede llegar a reducir considerablemente el nivel de riesgo general de la herramienta que se esté desarrollando.

Finalmente (ahora de verdad), me gustaría sintetizar un poco todo lo comentado anteriormente diciendo que está es una tecnología que hace muy poco tiempo ha dejado de estar en pañales y ha pasado a ser utilizada por muchísimas compañías distintas en muy poco tiempo es una herramienta con un potencial increíble que en un futuro cercano va a continuar sorprendiéndonos. Y en cuanto a lo relacionado con la

auditoría en este campo, creo que todavía es algo que puede estar construyéndose en este momento debido a que muchas de las ISO/IEC JTC 1/SC 42 están en desarrollo, pero no tengo dudas de que en el futuro va a tener una gran importancia.

Referencias:

[1] https://medium.com/machine-learning-in-practice/deep-learnings-permanent-peak-on-gartner-s-hype-cycle-96157a1736e

[2] https://www.iso.org/committee/6794475/x/catalogue/

[3] https://blog.twitter.com/engineering/en_us/topics/insights/2018/twittertensorflow.html

[4] https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/the-machine-learning-auditcrisp-dm-framework