9 - 4 | 2021

El uso de la IA para ciberseguridad

A utilização de IA para ciber-segurança

The use of AI for cybersecurity

Guillermo Fernández Rubio

Electronic version
URL: https://revistas.rcaap.pt/uiips/ ISSN: 2182-9608

Publisher
Revista UI_IPSantarém

Printed version
Date of publication: 31st December 2021 Number of pages: 7
ISSN: 2182-9608

Electronic reference

Rubio, G. (2021). *A utilizaço de IA para ciber-segurança. Nome do número.* Revista da UI_IPSantarém. *Edição Temática: Ciências Exatas e das Engenharias*. Número especial: Conferência Internacional Cooperação Internacional, multiculturalidade, trabalho colaborativo e ambientes mais inclusivos, sustentáveis e resilientes. 9(4), 91-97. https://revistas.rcaap.pt/uiips/

revistauiips@ipsantarem.pt
Complexo Andaluz,
Apartado 279
2001-904 Santarém

Revista da UI_IPSantarém – Unidade de Investigação do Instituto Politécnico de Santarém,
Vol. 9, N. º 4, 2021, pp. 91-97, Santarém
ISSN: 2182-9608
https://revistas.rcaap.pt/uiips/

EL USO DE LA IA PARA CIBERSEGURIDAD

A utilização de IA para ciber-segurança

The use of AI for cybersecurity

Guillermo Fernández Rubio
Universidad de Extremadura, España
210100059@esg.ipsantarem.pt

RESUMEN

A medida que los ataques cibernéticos presentan una mayor amenaza, la inteligencia artificial ofrece una serie de herramientas que pueden utilizarse para mejorar la ciberseguridad. A lo largo de este artículo podemos observar un gran numero de beneficios y desventajas de la inteligencia artificial en el ámbito de la ciberseguridad. En nuestros resultados hemos obtenido resultados positivos en ataques con Inteligencia artificial y también hemos obtenido resultados positivos a la hora de obtener información de ataques mediante el uso de la IA. Como conclusión, es necesario avanzar en la inteligencia artificial, ya que el creciente volumen y complejidad de los ataques requiere de mayores recursos para poder enfrentarlos. A su vez, los ciberdelincuentes también usaran la inteligencia artificial para realizar sus ataques.

Palabras clave: Amenazas, complejidad, Ciberseguridad, Inteligencia-Artificial, Recursos.

1 INTRODUCCIÓN

La inteligencia artificial en el ámbito de la ciberseguridad puede ser tanto beneficiosa, para realizar una buena defensa, investigación y práctica contra los ciberataques, como negativa, al ser una herramienta más para los ciberdelincuentes que pueden utilizarla para mejorar sus ataques.

Es importante saber que los propios sistemas de la IA, son susceptibles de ser atacados, por lo que no solo hay que crear una buena IA, sino también una IA segura, para evitar que los ciberdelincuentes se aprovechen de nuestros sistemas.

La IA es una tecnología en constante evolución y sus algoritmos permiten un aprendizaje automático, conocido como machine Learning, el cual, ayuda al sistema a adaptarse y aprender de los diferentes patrones.

2 INTELIGENCIA ARTIFICIAL EN APOYO DE LA CIBERSEGURIDAD

Gracias al desarrollo de la IA los diferentes profesionales de la ciberseguridad pueden realizar tareas de mayor complejidad como el manejo de la enorme cantidad de datos creados por la industria 4.0. Existen un gran número de de retos a los que se enfrenta la inteligencia artificial, desde

la protección de la privacidad, la defensa proactiva, identificación de comportamientos extraños, detección de amenazas etc.

Las tecnologías de IA, como el machine leargning y el procesamiento del lenguaje natural, recopilan información y brindan esta a los analistas, ayudandoles a conectar los puntos de amenaza.

ENISA (The European Union Agency for Cibersecurity, 2021) indica que debe seguir investigandose la utilización de IA en la inteligencia de ciberamenazas para reducir el número de pasos manuales en los análisis realizados y validar dichos análisis a lo largo del ciclo de la gestión y mitigación de los riesgos de la seguridad.

En la actualidad con el COVID-19 se ha mostrado un gran aumento de la capacidad de los cibercriminales para adaptarse al vulnerable teletrabajo y así poder acceder a los datos de sus empresas. Si las técnicas que han utilizado, que son las ya conocidas como phising, ocultación de malware e ingeniería social, se van combinando con la IA, cada vez serán más dificiles de detectar y tendrán un mayor éxito.

2.1 Abordar la inteligencia artificial en la ciberseguridad

Es necesario crear sistemas de IA seguros y justos para reducir el esfuerzo adicional que habrá que realizar en el futuro para resolver los problemas generados en caso de crear sistemas de IA que no sean seguros, debido a las amenazas que estos ofrecen para los ciberdelincuentes.

Para desarrollar, validar y desplegar sistemas de IA, se han recopilado una serie de aspectos que se deben tener en cuenta:

- Privacidad: Mantener la privacidad de los datos
- Equidad: que no favorezca determinadas salidas por sesgos implícitos.
- Trazabilidad: poder analizar los fallos del sistema.
- Robustez: hasta que punto podemos fiarnos del sistema.
- Fiabilidad: modelo fiable y si cambia.
- Causalidad: influir en la salida del modelo
- Explicabilidad y transpariencia: los usuarios deben entender el funcionamiento del modelo.
- Gobernanza del dato: licito, eficiente y eficaz de la información.

3 LA UTILIZACIÓN DE LA IA POR PARTE DE LOS CIBERATACANTES

Los sistemas de IA y ML proporcionan información automatizada mediante el análsis de grandes volúmenes de datos y el descubrimiento de patrones, esto nos ofrece unas predicciones, pero esto mismo es utilizado por los ciberdelincuentes para un beneficio indebido.

3.1 Deepfakes

Uno de los abusos más populares mediante el uso de la IA son los deepfakes, que implican diferentes tecnicas para crear o manipular el contenido visual y auditivo para que parezcan autenticos. Esto es muy útil en compañias de desinformación, llegando a millones de personas debido al uso actual de internet.

Un ejemplo que se volvio bastante viral, fue cuando se público un video de el ex presidente de los Estados Unidos, Obama, donde daba unas duras declaraciones. Por suerte, esto fue un experimento de la empresa *BuzzFeed* en 2018, que trabajaba con el director *Jordan Peele*, para mostrar al mundo el peligro de los Deepfakes.

El uso de los Deepfakes es utilizado por los ciberdelincuentes en el mundo de la pornografía por lo beneificioso que es, ya que ofrecen videos de celebridades que realmente no existen pero que con las técnicas de Deepfakes pueden engañar a una gran parte de usuarios.

3.2 Adivinación de contraseñas compatibles con AI

Con las técnicas de Machine Learning los ciberdelincuentes mejoran sus algoritmos para adivinar la contraseñas de usuarios. Con las redes neuronales y redes adversarias generativas, los ciberdelincuentes podrían analizar grandes conjuntos de contraseñas y variaciones de contraseñas que se ajusten a la distribución estadística.

3.3 Suplantación de identidad humana en plataformas de redes sociales

Los ciberdelincuentes quieren replicar el comportamiento humano, para eso, utilizan la IA, imitando esta el comportamiento humano y así poder realizar tráfico fraudulento y generar distintos flujos de datos, como podría ser en la plataforma Spotify, usando la IA para engañar y que un artista mejore sus estadísticas.

Existen numerosos foros donde se habla de la posibilidad de crear bots para distintas redes sociales o lugares con interés para los ciberdelincuentes, como por ejemplo, *blackhatworld*.

3.4 Hackeo apoyado por IA

Una de las formas de piratear hosts vulnerables es mediante el uso de la IA. Por ejemplo, Pwnagotchi 1.0.0, que es una herramienta para piratear Wi-Fi mediante ataques de desautenticación, esta herramienta es recompensada cuando el sistema anula la autenticación con éxito y así aprende a mejorar de forma autónoma.

4 MÉTODO

El método que hemos utilizado en primer lugar ha sido la recopilación de información de diferentes organizaciones, donde se explicaban y mostraban el uso de la IA en el ámbito de la ciberseguridad.

En el segundo apartado, hemos obtenido datos de diferentes informes de organizaciones, donde se muestran los intereses de las empresas en el uso de la IA para poder identificar amenazas.

Informe del instituto de Investigación Capgemini (Instituto de investigación de Capgemini, 2021)

Informe de Gartener (Gartener, 2021)

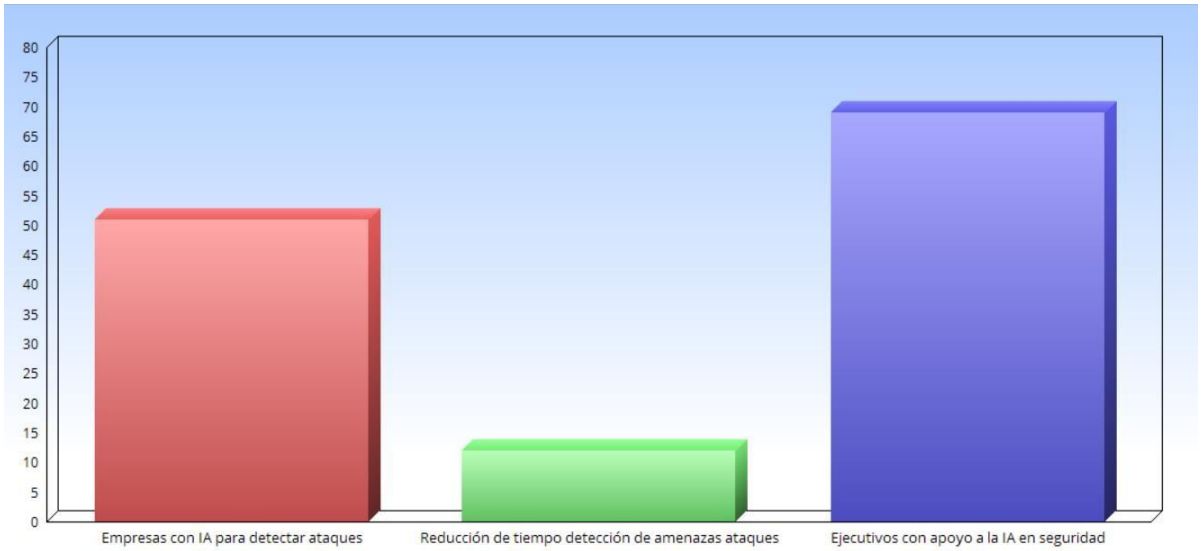
En tercer lugar, hemos utilizado una herramienta gratuita para la creación de DeepFakes, llamada DeepWord. Esta herramienta nos ha permitido crear con cierta facilidad y en línea, un clip en el que se vea a la persona que protagonizará el deepfake y una fuente de audio de la misma duración del video.

5 RESULTADOS

Los datos que hemos obtenido en el caso de los informes sobre el uso de la IA en ciberseguridad, han sido recogidos en el gráfico 1 y en el gráfico 2.

Imagen 1

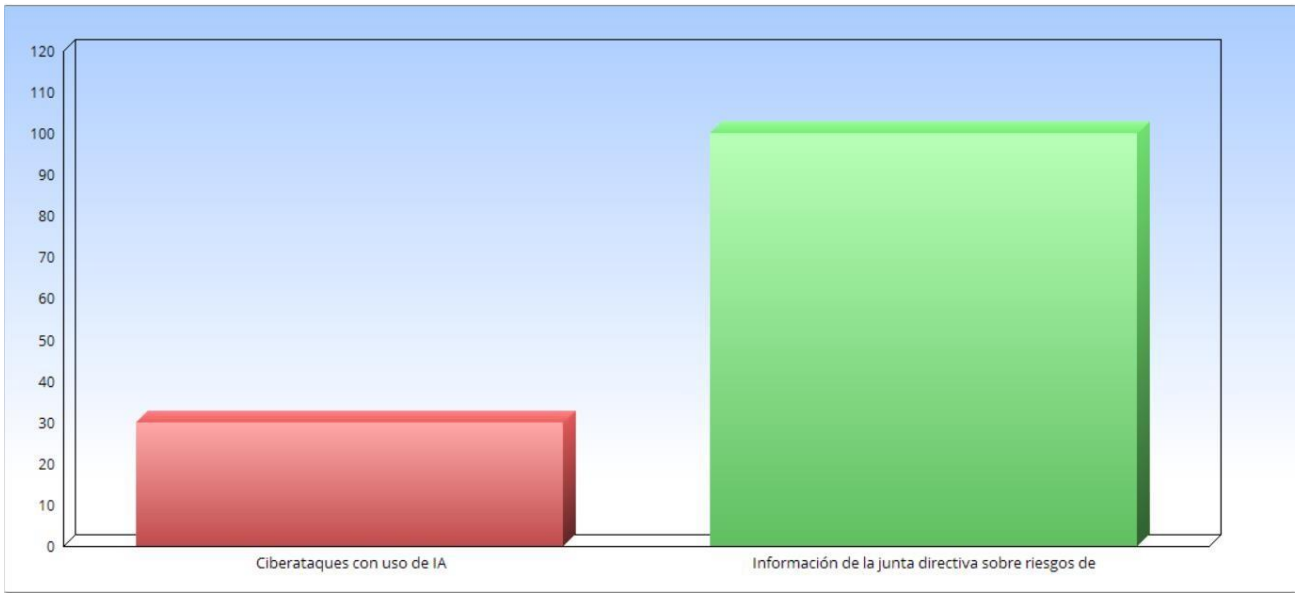
Informe del instituto de Investigación Capgemini



Notas: Representación en %

Gráfico 2

Informe Gartener

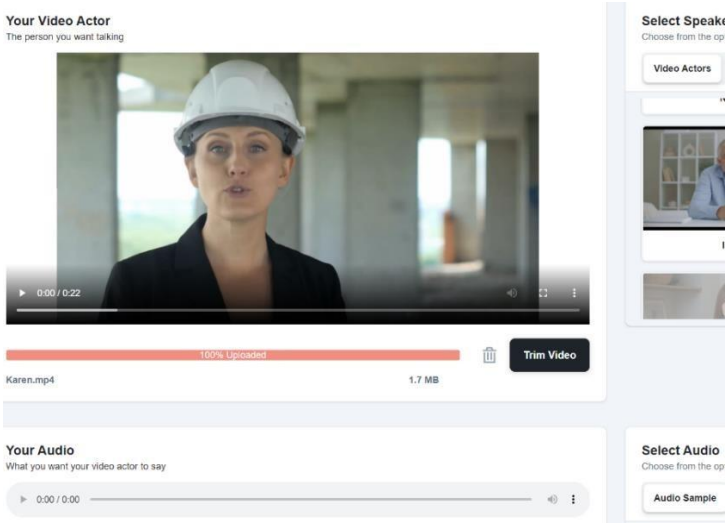


Notas: Representación en %

La utilización de la herramienta de DeepFake, llamada DeepWord, nos ha dado como resultado la creación de un clip del cual hemos utilizado nuestra voz y movimientos, en la cara de otra persona. En la imagen 1 se observa la creación de nuestro clip.

Imagen 2

Creación de DeepFake con DeepWord



6 DISCUSIÓN DE RESULTADOS

Los datos arrojados en el informe Capgemini (Instituto de investigación Capgemini, 2021) nos muestra el crecimiento de las empresas en el uso de la IA y la confianza de los ejecutivos en el desarrollo de esta IA para poder frenar las grandes perdidas de esfuerzo y dinero que suponen a las empresas los ataques de los ciberdelincuentes. Además nos muestra como la IA ahorraría tiempo, un 12%, en detectar las amenazas, que es una cantidad bastante grande para la importancia de esta tarea.

En cuanto al informe Gartener (Gartener, 2021), nos muestra como los ciberataques con el uso de la IA estan en auge, aumentando su porcentaje cada año. La evolución del 40% al 100% respecto a este año de que las grandes compañias tienen que informar a la junta directiva de los problemas de ciberseguridad nos muestra la grandisima importancia que tiene en nuestro día el desarrollo de esta área.

7 CONCLUSIÓN

La inteligencia artificial en el ámbito de la seguridad, nos ha demostrado que es algo importantísimo y que cada día evoluciona a más, sin embargo, vive en un constante equilibrio, entre los beneficios que aporta para que analistas, expertos en ciberseguridad puedan mejorar sus algoritmos y eficacia y sus desventajas, de como los ciberdelincuentes pueden aprovecharse de ella para realizar ataques más complejos y actividades fraudulentas.

Los datos que nos ofrecen los informes a día de hoy son interesantes y nos ofrecen una visión más clara sobre la inteligencia artificial en la ciberseguridad, sin embargo, siguen siendo algo complicados para el público común, ya que requieren de cierta base para poder entenderlos y que sus datos se vayan extendiendo al público.

Las herramientas de IA en temas de ciberseguridad, son bastante amplias, en el caso de nuestro árticulo, hemos utilizado una que ha sido muy fácil de usar, sin la necesidad de descargar nada y que su resultado ha sido realmente interesante, por lo que cada día, avanzamos más en

herramientas que pueden tener usos muy interesantes, pero tambien pueden ser aprovechados por personas con intenciones maliciosas.

8 REFERENCIAS

La ciberseguridad y su relación con la inteligencia artificial. (2020, Noviembre 10). En realinstitutoelcano. Retrieved from http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial

Inteligencia artificial (IA) en ciberseguridad. (2021, Agosto 10). En Grupo Fractalia. Retrieved from https://fractaliasystems.com/inteligencia-artificial-ia-en-ciberseguridad/

¿Qué es la ciberseguridad? (2008). En Cisco. Retrieved from https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

¿Qué es la Inteligencia artificial - IA? (2017). En Oracle. Retrieved from https://www.oracle.com/es/artificialintelligence/what-is-ai/

How CiberCriminals Misuse and abuse AI and ML(2020, Noviembre, 19) En Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/exploiting-ai-howcybercriminals-misuse-abuse-ai-and-ml

Reinventando la ciberseguridad con inteligencia artificial (2021) En Capgmini. Retrieved from https://www.capgemini.com/es-es/instituto-de-investigacion-de-capgemini/reinventando-laciberseguridad-con-inteligencia-artificial/

Create Videos of People Talking With AI (2021) En DeepWord. Retrieved from https://www.deepword.co/

Ciberseguridad y gestion de riesgos empresariales digitales (2021) En Gartner. Retrieved from https://www.gartner.es/es/tecnologia-de-la-informacion/insights/ciberseguridad

Crear gráficos en Línea (2021) En Chartgo. Retrieved from https://www.chartgo.com/index_es.jsp