Comunidad de Madrid

Medios de Comunicación

El Instituto Madrileño de Estudios Avanzados (IMDEA) Software ha desarrollado una solución para verificar la edición de contenidos

La Comunidad de Madrid crea técnicas de verificación para aumentar la seguridad en el uso de la Inteligencia Artificial

- Su aplicación en la IA y en el procesamiento de imágenes es más rápida y eficaz que los métodos actuales y es compatible con la confidencialidad
- También se pueden utilizar en procesos relacionados con la información financiera o la protección de datos personales

1 de mayo de 2024.- La Comunidad de Madrid desarrolla técnicas innovadoras de verificación para aumentar la seguridad en el uso de Inteligencia Artificial (IA) y el procesamiento de imágenes. El estudio, liderado por el Instituto Madrileño de Estudios Avanzados (IMDEA) Software, junto a la Universidad Carlos III de Madrid y NEC Laboratories Europe, ha creado una herramienta que mejora la computación verificable para detectar contenidos editados.

Este sistema comprende una familia de técnicas criptográficas que permiten obtener una garantía infalsificable de que algún tercero, como una empresa o un servidor en la nube, ha realizado un procesamiento correcto de los datos de un usuario. Así, puede demostrar si una imagen o un vídeo han sido editados, confirmar que una predicción realizada por IA proviene de un modelo auditado, o que en una decisión sobre solvencia crediticia sólo se ha utilizado información proporcionados por el cliente. Todo ello de manera compatible con la privacidad para garantizar su confidencialidad.

Los investigadores han introducido un protocolo que puede integrarse fácilmente en una cadena de procesamiento de datos para permitir la verificación completa de, por ejemplo, las predicciones realizadas por redes neuronales, que son la base de la mayoría de modelos de IA. El equipo ha realizado un prototipo de aplicación de sus sistemas de comprobación que supone una notable mejoría a las técnicas existentes, especialmente por su rapidez.

Estos resultados, generados en el marco del proyecto PICOCRYPT con una beca del Consejo Europeo de Investigación, no sólo mejoran la eficiencia y la escalabilidad de los sistemas de pruebas criptográficas, sino que también abren nuevas posibilidades para garantizar la integridad, equidad y privacidad de las tareas de procesamiento de datos.

El estudio lleva por título *Modular Sumcheck Proof with Applications to Machine Learning and Image Processing* y está liderado por el investigador de IMDEA Software, David Balbás.