Inteligencia Artificial para el Bien[1]
Webinar Series[2]

Con el propósito de generar concientización y compartir información relevante que puede ayudar a combatir el COVID-19 en nuestro país, integrantes del Laboratorio de Innovación e Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires[3] (www.ialab.com.ar) participaron del segundo seminario web organizado por las Naciones Unidas. El presente documento describe el rol de las aplicaciones móviles para el seguimiento de contactos, conforme a lo expuesto en dicho seminario.

COVID-19. Uso de teléfonos móviles e IA para el seguimiento de contactos respetando la privacidad[4]

El seguimiento de contactos es una respuesta clave de salud pública en la lucha contra brotes de enfermedades infecciosas como el COVID-19. Las tecnologías móviles proporcionan varias formas en las que se puede realizar el rastreo de contactos, incluido el uso de GPS, Bluetooth, antenas de teléfonos celulares y análisis de Big Data impulsados por IA para recopilar datos que ayuden a los tomadores de decisiones a comprender y administrar la propagación del COVID-19 dentro de sus comunidades.

Preservar la privacidad personal mientras se utiliza la tecnología móvil para abordar el COVID-19 es fundamental para mantener la confianza pública y proteger a las personas vulnerables en nuestro estado actual de crisis. Este episodio presenta a expertos clave que discuten acerca de la implementación de técnicas de preservación de la privacidad, como el cifrado homomórfico y soluciones para el monitoreo de contactos de teléfonos móviles.

Seguimiento de contactos

El rastreo de contactos consiste en encontrar a todos aquellos que tuvieron contacto con una persona diagnosticada medicamente con COVID-19 en los últimos 14 días.

---

[1] Inteligencia Artificial para el Bien -*AI for Good*- es la principal plataforma de las Naciones Unidas orientada a la acción global e inclusiva sobre IA. La Cumbre es organizada cada año en Ginebra por la UIT y busca conectar a los innovadores de IA con los propietarios de los problemas para acelerar el progreso hacia los Objetivos de Desarrollo Sostenible de las Naciones Unidas, liberando el potencial de la IA y otras tecnologías relacionadas.

[2] Webinar Series se compone de una serie de charlas, entrevistas y paneles gratuitos y en vivo, con expertos interdisciplinarios cuyas ideas y soluciones pueden ayudar a la humanidad a aprovechar la IA. Basados en la experiencia de la comunidad de AI for Good, estos seminarios web buscan compartir los últimos desarrollos en IA, ideas únicas y casos de uso prometedores sobre desafíos globales desde la salud hasta el medio ambiente y la reducción de las desigualdades.

[3] Se trata del primer Laboratorio de Innovación e Inteligencia Artificial en una Facultad de Derecho de América Latina. Ver: www.ialab.com.ar

[4] Panelistas: Thomas Wiegand, Profesor y Director Ejecutivo, Instituto Fraunhofer Heinrich Hertz y Kurt Rohloff, Profesor Asociado en NJIT y Cofundador de Duality Technologies. El Instituto Fraunhofer Heinrich Hertz está trabajando en una aplicación que almacena de manera anónima la proximidad y la duración de los contactos entre personas en dispositvos móviles.

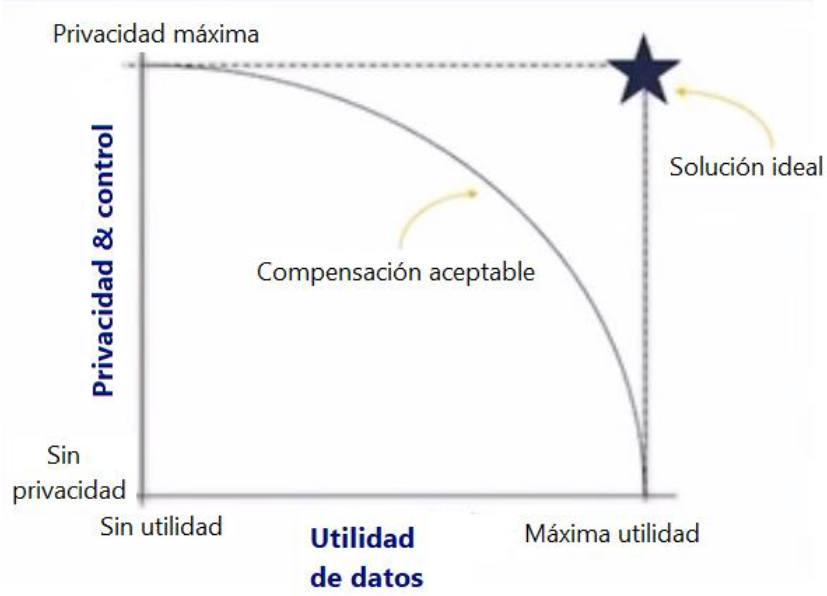
El seguimiento de contactos posibilita una respuesta rápida y efectiva, y permite descubrir nuevos casos rápidamente, aislar a la población y evitar una mayor propagación. Sin embargo, significa un desafío importante para compartir datos. Para lograr erradicar el COVID-19, el intercambio de datos es un paso vital para fortalecer nuestra respuesta colectiva.

Colaboración digital segura

-Las regulaciones de privacidad y las preocupaciones de propiedad intelectual han sido barreras.

-Los propietarios de datos y las agencias de salud han dudado en compartir la información debido a las normas de privacidad.

Para que el intercambio de datos sea posible, se necesita de la colaboración segura en el análisis de datos. A su vez, se deben atender cuestiones relativas a la privacidad, regulación, seguridad y secretos comerciales.



Tecnologías de mejora de la privacidad. Definiciones y resumen

Estas tecnologías son parte de una caja de herramientas utilizada para abordar diferentes problemas

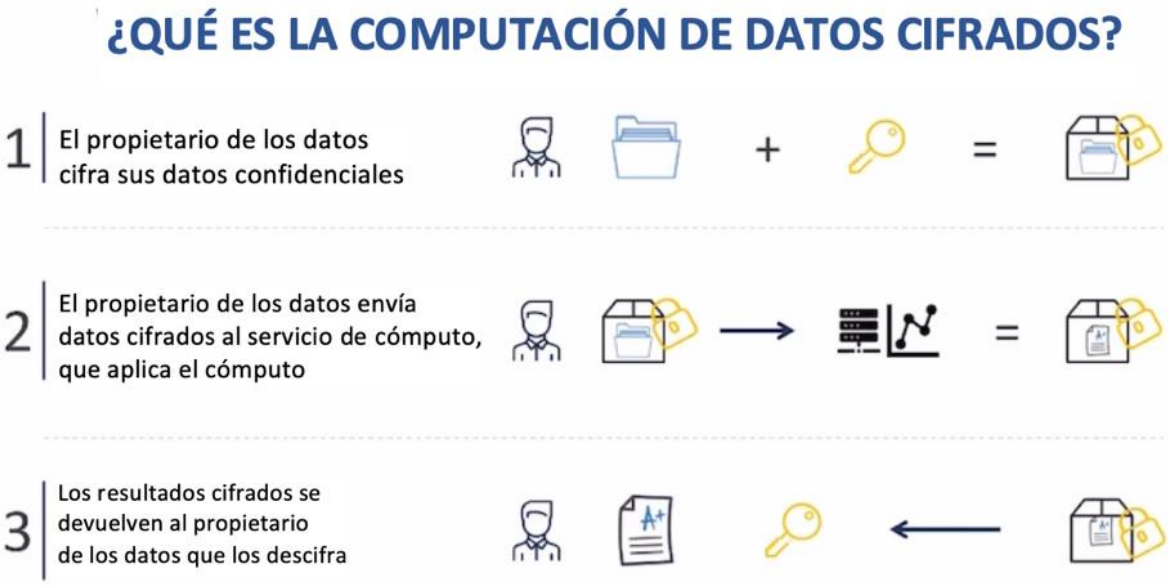
	Enclave de hardware seguro	Cómputo seguro de múltiples partes	Privacidad diferencial	Cifrado homomórfico
Definición	-Datos asegurados utilizando hardware seguro -Datos inaccesibles para cualquier proceso fuera del hardware seguro -Permite que las aplicaciones se ejecuten con datos sensibles	Permite a las partes realizar un cómputo conjunto de entradas individuales sin revelar datos subyacentes	Datos agregados que incluyen ruido generado aleatoriamente, lo que limita la capacidad de cada parte para realizar ingeniería inversa de entradas individuales	-Datos y/o modelos encriptados en reposo, en tránsito y en uso -Los cálculos se ejecutan en datos cifrados -Se puede combinar con otros métodos, como SMPC, para ofrecer enfoques híbridos
Uso típico	Ejecución de aplicaciones sobre datos sensibles en un hardware en entornos menos confiables (por ejemplo, nube)	Evaluación comparativa entre las partes colaboradoras donde la producción agregada es adecuada	Análisis de datos agregados cuando no se necesitan resultados individuales y precisos (por ejemplo, datos del censo)	Casos en los que se desea flexibilidad en el cómputo, cumplimiento normativo, precisión y seguridad
Inconvenientes	-Dependencia del hardware -Requiere modificaciones de software -Se ha demostrado que es susceptible de ataque	-El resultado del análisis es conocido por todas las partes y puede usarse para inferir datos sensibles -La implementación suele ser compleja -Normalmente requiere una comunicación intensa entre las partes, lo que genera altos costos	-Los resultados son direccionalmente correctos, pero no precisos -Número limitado y tipo de cálculos pueden ejecutarse debido al ruido agregado	Rendimiento más lento vs. cálculos en claro, normalmente el mejor para el procesamiento por lotes o "cálculo a escala humana"

AI for Good Webinar Series

IALAB

Tecnologías de mejora de la privacidad: técnicas de comparación

	Enclave de hardware Seguro	Computación segura de varias partes	Privacidad diferencial	Cifrado homomórfico
Hardware independiente	✗	✓	✓	✓
Cifrado de extremo a extremo	✗	✗	✗	✓
Resultados exactos para cálculos generales	✓	✓	✗	✓
Preciso para conocimientos a nivel individual	✓	✓	✗	✓
Soporte para delegación de acceso criptográfico	✗	✓	✗	✓
Permite la colaboración en múltiples conjuntos de datos	✓	✓	✓	✓



Privacidad protegida COVID-19. Seguimiento de contactos

Es necesario identificar a las personas expuestas a COVID-19 en función de su ubicación, sin exponer información de identificación personal. Para ello, se debe usar el cifrado homomórfico que permite analizar datos mientras están cifrados. De este modo, se podrá extraer información de los datos, sin exponer información confidencial.

A diferencia de las formas tradicionales de cifrado que aseguran los datos solo “en reposo” o “en tránsito”, el cifrado homomórfico asegura los datos mientras estos son utilizados. Además, este cifrado permite la realización de análisis, incluidos el aprendizaje automático y los modelos de IA para aplicar a los datos cifrados. Los resultados del cifrado homomórfico son los mismos que se hubieren obtenido en caso de que el análisis se hubiere realizado sobre datos desprotegidos.

El cifrado homomórfico se está desarrollando como un estándar de privacidad que permite conocer el valor de los datos y al mismo tiempo protege la privacidad. Gracias al mismo es posible desarrollar una funcionalidad para el seguimiento de contactos que protege a la privacidad y a la vez, permite a las autoridades sanitarias identificar la exposición del COVID-19 sin compartir información confidencial con proveedores de datos, ni visualizar información perteneciente a individuos no expuestos.

AI for Good Webinar Series

IALAB

Consulta segura 1

Entrada: identificador único (número de teléfono, correo electrónico) de personas infectadas y rango de fechas

Salida: ubicaciones, fechas y horas donde se pinchó dispositivos móviles

¿Cómo se mejora la privacidad?

Los proveedores de datos de ubicación no pueden ver los datos ingresados o recibidos por las autoridades sanitarias

Las autoridades sanitarias no pueden ver los datos relacionados con personas no expuestas.

Consulta segura 2

Entrada: ubicaciones, fechas y horas donde se pinchó el dispositivo móvil

Salida: individuos en el mismo lugar y al mismo tiempo que individuos infectados

¿Cómo se mejora la privacidad?

Los proveedores de datos de ubicación no pueden ver los datos ingresados o recibidos por las autoridades sanitarias

Las autoridades sanitarias no pueden ver los datos relacionados con personas no expuestas.

Acción

Las autoridades sanitarias pueden:

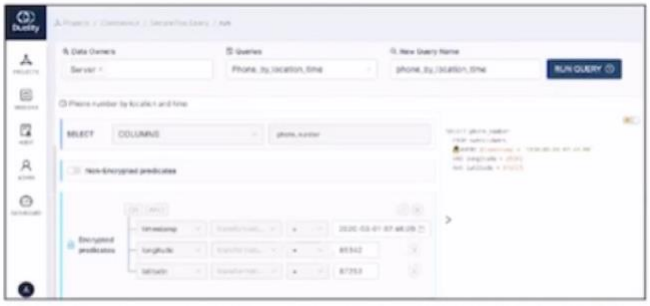
. Contactar a personas sospechosas de exposición

. Contactar a empresas expuestas

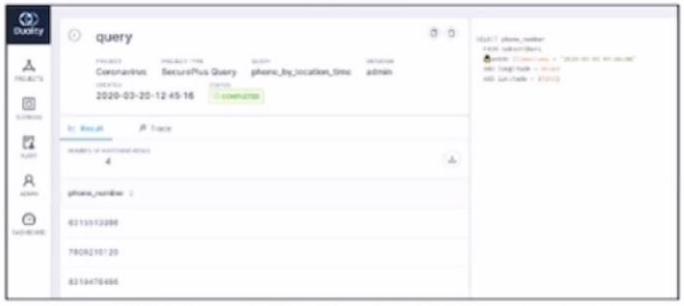
.Mejorar la coordinación entre los centros de salud, el cumplimiento de las leyes y las agencias gubernamentles

CONSULTA SEGURA 2: Dada la información de ubicación de un caso COVID-19 confirmado, muestra quién más estaba en el mismo lugar al mismo tiempo

Entrada



Salida



Dados los resultados de la consulta anterior, la autoridad de atención médica puede ingresar las ubicaciones y los horarios en que se encontraban las personas que confirmaron tener COVID-19.

Dados los resultados de la consulta anterior, la autoridad de atención médica puede ingresar las ubicaciones y los horarios en que se encontraban las personas que confirmaron tener COVID-19.

¿Cómo se mejora la privacidad?

- Los proveedores de datos de ubicación no pueden ver los datos ingresados o recibidos por las autoridades sanitarias
- Las autoridades sanitarias no pueden ver los datos relacionados con personas que no estuvieron potencialmente expuestas a COVID-19

AI for Good Webinar Series

IALAB

Resumen y acciones

Agencias de Salud

- Pueden realizar seguimiento de contactos mientras se preserva la privacidad de los casos confirmados y posibles infectados de COVID '19
- No pueden acceder a datos sobre personas que no están potencialmente expuestas a COVID-19
- Puede utilizar la información para contactar a personas y negocios que pueden haber estado expuestas, coordinar la respuesta con el gobierno local, la policía y la atención médica

Proveedores de datos

- Pueden ayudar a las agencias de atención médica a identificar personas y negocios expuestos a COVID-19
- No pueden ver datos sobre personas confirmadas o posibles infectados de COVID-19
- Proteger la privacidad de las personas que no estén potencialmente expuestas a COVID-19