nota de prensa

Una tecnología clave para la creación de soluciones digitales que preserven la privacidad y la seguridad de la información de los usuarios.

IMDEA Software y BBVA se alían para investigar técnicas de criptografía avanzada

4 de mayo de 2020. Madrid. A través de esta alianza, el Instituto IMDEA Software y BBVA han creado un marco común de trabajo para investigar el uso de esta tecnología en el desarrollo de soluciones digitales que **permitan aprovechar el potencial de los datos**, y al mismo tiempo, garanticen que se preserva la privacidad, el anonimato y la seguridad de la información de los usuarios.

El acuerdo cobra especial relevancia en el contexto actual, marcado por la crisis del coronavirus, que está poniendo de manifiesto la importancia de contar con **sistemas robustos que permitan salvaguardar la privacidad** y seguridad de los datos. Por un lado, debido al incremento de ciberataques producido en las últimas semanas en los que los cibercriminales están aprovechando el mayor uso de canales digitales que realizan los usuarios durante el periodo de confinamiento. Y por otro lado, debido al interés que ha despertado la creación de 'apps' de seguimiento del COVID-19 que respeten la privacidad de los datos, para las que tecnologías de este tipo podrían ser de gran utilidad.

Con esta nueva alianza, ambas entidades explorarán la aplicación en el sector financiero de una serie de técnicas criptográficas que permiten que los datos puedan ser analizados y compartidos sin exponer su contenido a terceros, gracias a algoritmos, protocolos y sistemas de encriptación. Estas tecnologías, conocidas como PET, por sus siglas 'Privacy-Enhancing Technologies' (o técnicas de mejora de la privacidad), son uno de los campos de especialidad del Instituto IMDEA Software, así como una de las áreas de interés en las que BBVA investiga a través del departamento de Investigación y Patentes.

Dentro de este grupo de tecnologías, una de las que presenta mayor potencial –y será principal objeto de estudio del nuevo equipo de trabajo–, es la 'Prueba de Conocimiento Nulo', o ZKP por sus siglas en inglés ('Zero-Knowledge Proofs'). Esta tecnología emplea algoritmos criptográficos para facilitar que sea posible verificar la veracidad de una información, sin necesidad de compartir los datos que la componen. De esta forma, puede ayudar a **crear soluciones basadas en datos**, en las que la información sensible de los clientes no se vea expuesta a terceros (ya que para probar que son verdaderos, no es

software.imdea.org
Instituto IMDEA Software
Campus de Montegancedo, s/n · 28223 Pozuelo de Alarcón · Madrid, España
+34 91 101 22 02 fax +34 91 101 13 58 software@imdea.org

necesario compartir los datos en sí).

Gracias al acuerdo, ambas entidades suman sus capacidades y conocimiento en estas áreas con el objetivo de que la investigación **pueda traducirse en avances tangibles** que permitan que los beneficios de esta tecnología se trasladen al sector financiero, así como al mundo empresarial, la comunidad científica y la sociedad en su conjunto.

Para ello, en una primera fase, el equipo conjunto investigará cómo **resolver algunos de los actuales retos** a los que aún se enfrenta el despliegue de esta tecnología con el objetivo de compartir los resultados con la comunidad científica para favorecer el avance de esta disciplina. Algunos de estos retos son su integración con los actuales sistemas de comunicación que emplean las compañías o la ausencia de estándares comunes para el uso de protocolos criptográficos, que dificulta su adopción a gran escala.

El Instituto IMDEA Software y BBVA también trabajarán en una serie de casos de uso reales identificados en el sector financiero, así como en el **desarrollo de prototipos viables** que puedan incorporarse en los servicios y productos digitales que se ofrecen a los clientes de BBVA.

“Existe una necesidad creciente de desarrollar soluciones tecnológicas que nos permitan preservar la privacidad de la información que compartimos al consumir servicios digitales en nuestro día a día; y en BBVA vemos un gran potencial en estas tecnologías para hacerlo posible. Esta necesidad se ha hecho aún más tangible **a raíz de la crisis del COVID-19**, que está poniendo de manifiesto la necesidad de contar con sistemas robustos de protección de nuestros datos, ante el crecimiento de los ciberataques y el uso de aplicaciones que registran los datos de los usuarios para realizar seguimientos de la enfermedad que han surgido en algunos países”, explica Carlos Kuchkovsky, responsable de Investigación y Patentes en BBVA. “Ahora, gracias a esta colaboración, vamos a poder ampliar nuestras capacidades para investigar en este área de conocimiento y aplicarlas en el banco para que sus ventajas lleguen a nuestros clientes”, ha añadido.

“Hasta hace poco, estas técnicas criptográficas se consideraban sólo de interés teórico. En los últimos años hemos visto enormes avances que pueden hacerlas aplicables a algunos escenarios prácticos, pero aún quedan varios desafíos por delante: la eficiencia y la integración en sistemas más grandes, entre otros”, explica el investigador posdoctoral del en el Instituto IMDEA Software, Antonio Faonio. El investigador Dario Fiore, ‘Associate Research Professor’ del Instituto que también formará parte de esta alianza, comenta que “esta colaboración puede ayudarnos -tanto a nosotros como a la comunidad científica- a transferir esta tecnología a los agentes industriales pertinentes y a identificar los problemas que es preciso abordar para alcanzar este objetivo”.

Instituto IMDEA Software
Campus de Montegancedo, s/n · 28223 Pozuelo de Alarcón · Madrid, España
+34 91 101 22 02 fax +34 91 101 13 58 software@imdea.org

instituto IMDEA software

nota de prensa

Casos de uso

BBVA lleva tiempo investigando la aplicación de estas tecnologías, y en concreto la tecnología ZKP, en el sector financiero; y ya ha identificado distintos escenarios en los que presenta grandes ventajas. Por su parte, el Instituto IMDEA Software cuenta con algunos de los expertos más reconocidos del panorama internacional en este campo, que investigan activamente la constante mejora de la tecnología ZKP.

En términos generales, la tecnología podría servir para facilitar que las entidades financieras puedan verificar que una información necesaria para la comercialización de un producto o servicio es verdadera (como el salario o la edad de un cliente), sin necesidad de exponer datos sensibles. De la misma forma, la tecnología también podría utilizarse para que las entidades financieras faciliten que los usuarios compartan con terceros pruebas digitales que certifiquen su información financiera, sin tener que compartir los datos.

En el ámbito de la identidad, la tecnología también podría emplearse para desarrollar sistemas de autentificación sin riesgo de que la información sea robada, ya que para probar la identidad no es necesario compartir ningún dato personal.

Para más información:

Instituto IMDEA Software
Blanca Gutiérrez
Tel. 680 99 06 72
blanca.gutierrez@imdea.org

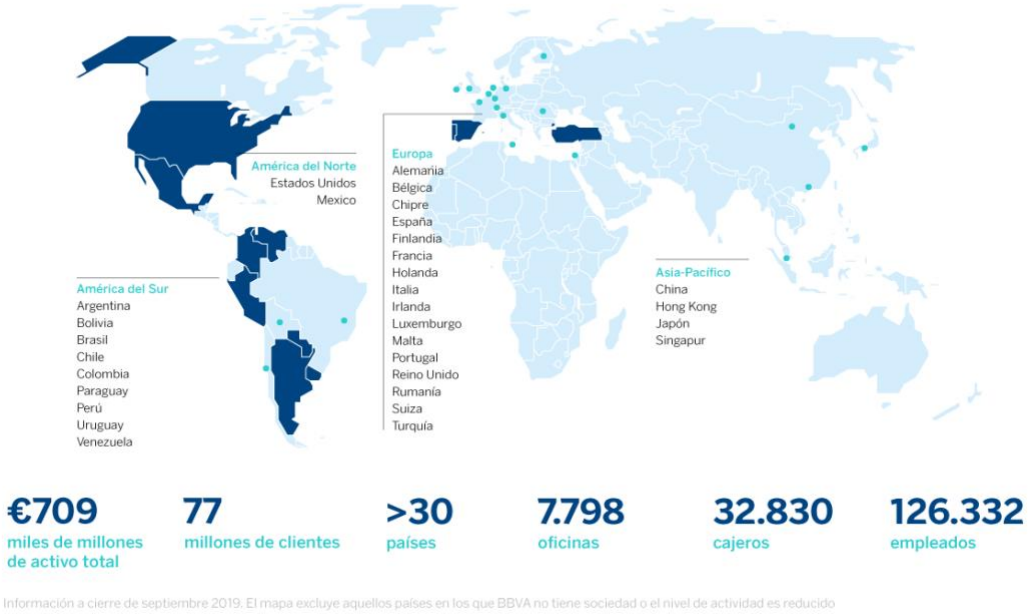
BBVA
Teresa Alameda
Tel. 619 27 40 63
teresa.alameda@bbvacreative.com

nota de prensa

Acerca del Instituto IMDEA Software

El Instituto IMDEA Software es uno de los 7 centros de investigación que forman parte de la iniciativa IMDEA, creada por la Comunidad de Madrid en 2006. Recluta al mejor talento internacional para estar a la vanguardia de la investigación y lograr que el software sea seguro, fiable y eficiente.

Acerca de BBVA



BBVA es un grupo financiero global fundado en 1857 con una visión centrada en el cliente. Tiene una posición de liderazgo en el mercado español, es la mayor institución financiera de México y cuenta con franquicias líder en América del Sur y la región del Sunbelt en Estados Unidos. Además, es el primer accionista de Garanti BBVA, en Turquía. Su propósito es poner al alcance de todos las oportunidades de esta nueva era. Este propósito está centrado en las necesidades reales de los clientes: proporcionar las mejores soluciones y ayudarles a tomar las mejores decisiones financieras, a través de una experiencia fácil y conveniente. La entidad se asienta en unos sólidos valores: el cliente es lo primero, pensamos en grande y somos un solo equipo. Su modelo de banca responsable aspira a lograr una sociedad más inclusiva y sostenible.

software.imdea.org

Instituto IMDEA Software
Campus de Montegancedo, s/n · 28223 Pozuelo de Alarcón · Madrid, España
+34 91 101 22 02 fax +34 91 101 13 58 software@imdea.org