Los desarrolladores detrás del navegador web de código abierto Brave, revelaron un nuevo sistema de consulta y recuperación de datos que preserva la privacidad denominado FrodoPIR.

La idea, según la compañía, es utilizar la tecnología para desarrollar una amplia gama de casos de uso, como navegación segura, verificación de contraseñas contras bases de datos violadas, verificación de revocación de certificados y transmisión, entre otros.

El esquema se llama FrodoPIR porque *«el cliente puede realizar consultas ocultas al servidor, tal como Frodo permaneció oculto para Sauron»,* una referencia a los personajes de El señor de los anillos de RR Tolkien.

PIR, abreviatura de recuperación de información privada, es un protocolo criptográfico que permite a los usuarios (también conocidos como clientes) recuperar una parte de la información de un servidor de base de datos sin revelar a su propietario qué elemento se seleccionó.

En otras palabras, el objetivo es poder consultar una plataforma para obtener información (por ejemplo, videos de educación) sin permitir que el proveedor de servicios infiera del historial de búsqueda de un solo usuario para ofrecer recomendaciones personalizadas o anuncios dirigidos según los criterios de búsqueda.

Una forma de lograr esto es mediante el uso de un enfoque llamado cifrado homomórfico, que permite que el cálculo se realice de forma directa en los datos cifrados sin necesidad de acceder a una clave privada.

Pero un problema común que afecta a estos métodos es que son *«caros en términos de ancho de banda o de tiempo necesario para procesar cada consulta del cliente»*, lo que los hace prohibitivos para las implementaciones en el mundo real.

Ahí es donde interviene FrodoPIR. Se trata de dos fases, un paso preparatorio fuera de línea y un paso en línea en el que el cliente transmite consultas cifradas al servidor.

Posteriormente, el servidor opta por devolver un valor positivo o negativo dependiendo de si la consulta se encuentra o no en la base de datos sin saber qué está consultando realmente el usuario.

> *«En términos de rendimiento para una base de datos de 1 millón de elementos KB, FrodoPIR requiere <1 segundo para responder la consulta de un cliente, tiene un factor de aumento del tamaño de respuesta del servidor de >3.6x y los costos financieros son ~$1 para responder a las consultas de los clientes»*, dijo Brave en una descripción de GitHub del proyecto.

Google lanza dos tecnologías Open Source de mejora de la privacidad (PET)

El desarrollo se produce cuando Google dijo que está abriendo dos tecnologías de mejora de la privacidad (PET) como parte de sus esfuerzos continuos para democratizar el acceso a técnicas más allá del aprendizaje federado y la privacidad diferencial.

Esto consiste en una nueva herramienta de aprendizaje automático llamada Magritte, que está diseñada para desenfocar objetos como matrículas presentes en videos, así como mejoras en la eficiencia de su transpilador de cifrado totalmente homomórfico (FHE).

El transpiler, también conocido como compilador o traductor de fuente a fuente, está diseñado para ejecutar consultas basadas en computación sobre información cifrada sin ningún acceso a datos de identificación personal.

Los PET *«brindarán a la comunidad de desarrolladores en general (investigadores, gobiernos, organizaciones sin fines de lucro, empresas y más) nuevas formas de implementar y mejorar*

las funciones de privacidad en su propio trabajo», dijo Google.