Secure and Functional Encrypted Databases

SaFED

Appel : APG 2019

Année : 2019-2023

Instrument : JCJC

Contact : brice.minaud@inria.fr

COORDINATEUR : Brice Minaud

PARTENAIRE : Inria

Résumé :
Les bases de données chiffrées permettent d'interagir avec des bases de données stockées dans le cloud, tout en maintenant la confidentialité des données vis-à-vis du serveur hôte. Ce project vise à faire progresser l'état de l'art dans ce domaine, à la fois en termes de sécurité et de fonctionnalité.

CONTEXTE

Lorsque nous utilisons un service de messagerie comme WhatsApp ou Slack, nos communications sont stockées dans le cloud. Nous voudrions pourtant qu'elles restent privées. De même, une entreprise peut vouloir déléguer le stockage de sa base de données client, tout en souhaitant qu'elle reste confidentielle.

Cela implique de chiffrer les données. Dès lors, impossible pour le serveur qui stocke les données d'interagir avec elles. Comment peut-il alors traiter les requêtes du client sur la base de données ?

Le but du « chiffrement avec recherche » (**Searchable Encryption**, ou **SE**) est de résoudre ce problème.

OBJECTIFS

Il n'existe pas aujourd'hui de solution pleinement satisfaisante en SE, malgré un intérêt considérable de la part de l'industrie. Toute construction de SE est un compromis entre performance, sécurité et fonctionnalité. Notre objectif est d'améliorer ces compromis dans ces trois dimensions.

RÉSULTATS

En étudiant l'efficacité de SE, notamment sur des disques Flash (SSD), nous avons introduit un nouveau critère de performance pour SE. Depuis, plusieurs résultats nous font penser que cette notion est la « bonne » notion :

- Tethys : première construction de SE statique optimale à la fois en débit en en stockage sur SSD (surcoûts constants par rapport à une base non chiffrée !).
[CRYPTO 2021, avec Bossuat, Bost, Fouque et Reichle.]

- Local[SSE] : construction de SE la plus efficace asymptotiquement, utilisant des techniques développées pour notre nouvelle notion. *[En soumission]*

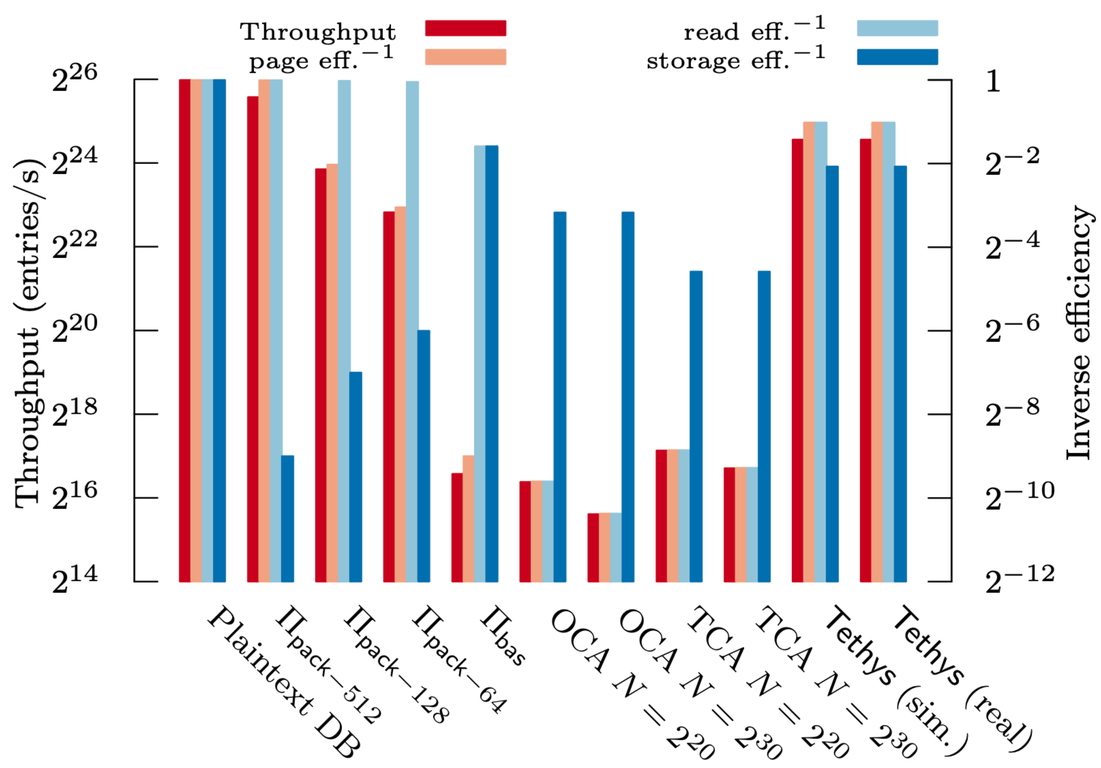

Figure : performance de Tethys, en débit et en stockage.

- Hermes : première construction de SE efficace en I/O qui soit *forward-secure* (propriété de sécurité importante), utilisant ces mêmes techniques. [*En soumission]*

Cette lignée de résultats devrait permettre d'améliorer la performance et la sécurité des bases de données chiffrées. Elle fait aussi le lien avec des questions théoriques intéressantes, surtout combinatoires.

Nous avons aussi travaillé sur des techniques permettant de limiter fortement les informations que le serveur peut déduire à partir des accès du client à la base de données. De telles techniques, appelées *ORAM*, existent : nous avons montré comment les adapter pour travailler avec des objets de taille variable, utiles en SE.
[*Article prévu pour soumission mi-février.]*

Travaux à venir : seuls les cas d'usage les plus simples sont aujourd'hui réalisables en SE avec un tant soit peu d'efficacité et de sécurité. Nous voulons développer de nouveaux modèles : recherches plus riches, requêtes sur des graphes chiffrés (réseaux sociaux), etc.