«EXÉCUTIONS DE REQUÊTES RESPECTUEUSES DE LA VIE PRIVÉE PAR UTILISATION DE COMPOSANTS MATÉRIELS SÉCURISÉS» PAR QUOC-CUONG TO

Présentée par : Quoc-Cuong To Discipline : informatique Laboratoire : DAVID

Résumé :
Les applications actuelles, des systèmes de capteurs complexes (par exemple auto quantifiée) aux applications de e-commerce, acquièrent de grandes quantités d' informations personnelles qui sont habituellement stockées sur des serveurs centraux. Cette quantité massive de données personnelles, considéré comme le nouveau pétrole, représente un important potentiel pour les applications et les entreprises. Cependant, la centralisation et le traitement de toutes les données sur un serveur unique, où elles sont exposées aux indiscrétions de son gestionnaire, posent un problème majeur en ce qui concerne la vie privée. Inversement, les architectures décentralisées aident les individus à conserver le plein de contrôle sur leurs données, toutefois leurs traitements en particulier le calcul de requêtes globales deviennent complexes. Dans cette thèse, nous visons à concilier la vie privée de l'individu et l'exploitation de ces données, qui présentent des avantages manifestes pour la communauté (comme des études

statistiques) ou encore des perspectives d’affaires. Nous promouvons l'idée de sécuriser l'acquisition des données par l'utilisation de matériel sécurisé. Grâce à ces éléments matériels tangibles de confiance, sécuriser des protocoles d'interrogation distribués permet d'effectuer des calculs globaux, tels que les agrégats SQL, sans révéler d'informations sensibles à des serveurs centraux.
Cette thèse étudie le sous-groupe de requêtes SQL sans jointures et montre comment sécuriser leur exécution en présence d'attaquants honnêtes-mais-curieux. Cette thèse explique également comment les protocoles d'interrogation qui en résultent peuvent être intégrés concrètement dans une architecture décentralisée. Nous démontrons que notre approche est viable et peut passer à l'échelle d'applications de la taille d'un pays par un modèle de coût et des expériences réelles sur notre prototype, SQL/AA.

Abstract :

Current applications, from complex sensor systems (e.g. quantified self) to online e-markets acquire vast quantities of personal information which usually end-up on central servers. This massive amount of personal data, the new oil, represents an unprecedented potential for applications and business. However, centralizing and processing all one?s data in a single server, where they are exposed to prying eyes, poses a major problem with regards to privacy concern. Conversely, decentralized architectures helping individuals keep full control of their data, but they complexify global treatments and queries, impeding the development of innovative services. In this thesis, we aim at reconciling individual's privacy on one side and global benefits for the community and business perspectives on the other side. It promotes the idea of pushing the security to secure hardware devices controlling the data at the place of their acquisition. Thanks to these tangible physical elements of trust, secure distributed querying protocols can reestablish the capacity to perform global computations, such as SQL aggregates, without revealing any sensitive information to central servers. This thesis studies the subset of SQL queries without external joins and shows how to secure their execution in the presence of honest-but-curious attackers. It also discusses how the resulting querying protocols can be integrated in a concrete decentralized architecture. Cost models and experiments on SQL/AA, our distributed prototype running on real tamper-resistant hardware, demonstrate that this approach can scale to nationwide applications.