B. Mitschang et al. (Hrsg.): Datenbanksysteme für Business, Technologie und Web (BTW 2017),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 23

Confidentiality à la Carte with Cipherbase

Donald Kossmann[1]

Abstract

Organizations move data and workloads to the cloud because the cloud is cheaper, more agile, and more secure. Unfortunately, the cloud is not perfect and there are some fundamental tradeoffs that need to be made in the cloud. The Cipherbase project studies the tradeoffs between confidentiality and functionality that arise when state-of-the-art cryptography is combined with databases in the cloud: The more operations that are supported on encrypted data, the more information that can be leaked unintentionally. There has been a great deal of work studying these tradeoffs in the specific context of property-preserving encryption techniques. For instance, deterministic encryption can support equality predicates directly over encrypted data, but it is also vulnerable to inference attacks. This talk discusses the tradeoffs that arise in a more general context when trusted computing platforms such as FPGAs or Intel SGX technology are used to process encrypted data.

Joint work with Arvind Arasu, Ken Eguro, Raghav Kaushik, Ravi Ramamurthy and the SQL Server Security Team.

[1] Microsoft Corporation, donaldk@microsoft.com