Thesis B.Sc.

Thesis M.Sc.

Analysis of Performance and Functionality of Cryptographic Databases

Motivation

Cryptographic databases allow the use of a database in the cloud while the data is encrypted. There are a variety of different options on how to achieve this. Fully homomorphic encryption allows to compute operations on encrypted data, yet it is extremely expensive. Cryptographic databases usually follow simpler approaches. Another option is to move the intelligence of the database operations to the client and server is mostly a secure storage and access provider. ZeroDB which we have already started to analyze follows such an approach. The next option is to use weaker and deterministic forms of encryption which allow the server to do a variety of select statements on the encrypted data.

In previous work we have already compared zeroDB, ZODB, and mysql. The comparison was based on certain select statements. The support of more types of statements would be desirable.

Your Task

- Study related work and previous work
- Extend our measurements with other kinds of queries
- Support an additional crypto database (e.g. from SafeCloud project)
- Analyze functionality supported
- Analyze performance as above

Contact

Heiko Niedermayer   niedermayer@net.in.tum.de
TBA