Suche in verschlüsselten Daten

April 2024

Die Gründe, warum Daten gesichert werden müssen, sind vielseitig. Die Daten können personenbezogene Information oder wertvolle Firmengeheimnisse enthalten. Eine der wichtigsten Schutzmaßnahmen ist dabei die Verschlüsselung, sowohl beim Transport über teils öffentliche Netzwerke wie dem Internet oder der Speicherung bei beispielsweise externen Cloudanbietern.

Selbstverständlich müssen die Daten später analysiert und wieder ausgelesen werden können. Hier offenbart sich ein entscheidender Nachteil gegenüber klassischen, lokalen Datenbanksystemen. In letzteren ist es möglich, mit geschickten Abfragen (SQL-Queries), gezielt Daten zu selektieren und zu filtern. Aber was, wenn der Datenbankserver die Daten nicht lesen können soll?

Um die Suche auch in verschlüsselten Daten zu ermöglichen, wurden unterschiedliche Verfahren entwickelt, welche unterschiedliche Arten der Suche erlauben. Die Möglichkeiten reichen von einfachen Stichwortsuchen bis zu Suchen nach Wertebereichen. Mit steigender Funktionalität erhöht sich dabei jedoch auch die Komplexität. Leider gibt es aktuell keine quantitativen Abschätzungen, die die "Suchbarkeit" dem Mehraufwand der Verschlüsselung gegenüberstellen. Dies soll nun im Rahmen einer studentischen Arbeit erfolgen.

Die Arbeiten umfassen dabei unter anderem folgende Aufgaben:

- Design eines Datenbanklayouts, welches die Suche in verschlüsselten Daten erlaubt.
- Entwicklung eines Testdatengenerators, mit dem suchbare, verschlüsselte Daten erzeugt werden können. Die Menge an Attributen, nach denen gesucht werden können soll, soll dabei flexibel einstellbar sein.
- Entwicklung und Durchführung von Testfällen zur Bewertung der Skalierbarkeit unterschiedlicher Verfahren zur Suche in verschlüsselten Daten.

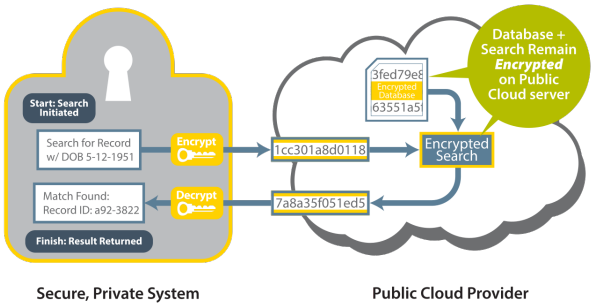

Figure 1: Beispielhaftes Konzept zur Suche in verschlüsselten Daten [1]

Kontakt: Prof. Dr.-Ing. Ralf Tönjes (`r.toenjes@hs-osnabrueck.de`) Raum UA 0308
Marten Fischer (`m.fischer@hs-osnabrueck.de`) Raum UA 0314

[1] https://www.bittware.com/de/resources/homomorphic-encryption/