Härtung von Bloom-Filtern zum Einsatz in PPRL-Protokollen

Praktikumsthema/Bachelorthema

Beschreibung

Privacy-preserving record linkage (PPRL) ist eine Art der Datenverknüpfung, die den Abgleich von Daten über diverse Datenquellen an verschiedenen Orten hinweg ermöglicht. Im medizinischen Kontext ist oft das Verknüpfen von Patientendaten über Institutionsgrenzen gewünscht. Dabei sind hohe Anforderungen an den Schutz dieser Daten zu stellen. Innerhalb des letzten Jahrzehnts haben sich hierfür Bloom-Filter als praktische Datenstruktur durchgesetzt. Im Idealfall erlauben sie die Unkenntlichmachung personenbezogener Daten ohne dabei die Vergleichbarkeit annähernd gleicher Datensätze zu beeinträchtigen.

Mit steigender Popularität von Bloom-Filtern steigen auch die Sicherheitsanforderungen. Die meisten PPRL-Protokolle auf Basis von Bloom-Filtern sind anfällig für Angriffe, die auf die ursprünglichen Personendaten zurückschließen lassen. Ebenso existieren eine Vielzahl von Empfehlungen für das Härten solcher Protokolle. Das Praktikums- bzw. Bachelorthema soll der Erschließung und Implementierung solcher Methoden dienen.

Ziele

- Erschließung der aktuellen Literatur zu PPRL-Verfahren basierend auf Bloom-Filtern bezüglich deren Sicherheitsaspekte und deren Härtung gegenüber kryptoanalytischen Angriffen
- Implementierung solcher Härtungsverfahren in Java und Auswertung hinsichtlich der Qualität und Sicherheit des Datenabgleichs

Voraussetzungen

- Gute Programmierkenntnisse
- Gute Kenntnisse der Programmierung in Java
- Grundlegende Kenntnisse über kryptografische Verfahren (v.a. Hash-Funktionen, HMAC, gängige Angriffe auf kryptografische Protokolle z.B. Frequency Attacks)
- Selbstständige Arbeitsweise beim Erschließen der aktuellen Literatur bzgl. PPRL
- Wünschenswert: Grundkenntnisse in der Verwendung von Git, Docker und Maven