Private Information Retrieval

Ida Hönigmann

April 6, 2020

Abstract

1 Idee

In diesem Projekt wird ein System entwickelt bei dem Clients Nachrichten von verschiedenen Servern abfragen können. Die Besonderheit liegt in der Sicherheit, die dem Client gewährleistet wird: keiner der Server weiß welche Nachricht der Client lesen möchte.

Eine Möglichkeit diese Sicherheit umzusetzen ist es den Client alle Nachrichten abfragen zu lassen. Dieses Projekt wählt allerdings einen anderen Ansatz, der eine geringere Menge an Daten, die übertragen werden müssen ermöglicht. Der Nachteil ist, dass ein Client jeweils Anfragen an zwei Server stellen muss. Daher müssen zumindest zwei Server existieren, um Nachrichten empfangen zu können.

2 Anwendungsfälle

Dieses System ist für alle Systeme der Form von Servern, die Clients Nachrichten anbieten anwendbar.

Denkbar wäre zum Beispiel eine solche Lösung bei Daten zu Krankheiten. Wenn ein Benutzer nach einer Krankheit sucht, von der er weiß oder befürchtet diese zu haben, möchte er eventuell nicht, dass der Betreiber des Servers Kenntnis davon hat. Das gilt jedoch auch für Personen, die die Krankheit nicht haben und Informationen darüber erhalten wollen. Es könnte angenommen werden, dass sie die Krankheit besitzen, da sie ja danach gesucht haben.

Ein zweiter Anwendungsfall wäre ein Online-Nachrichtendienst. Oft wird nicht dediziert das Verhalten der Nutzer analysiert, sondern nur Logdaten gesammelt um Analysen über die Auslastung der Systeme zu erstellen oder falls ein Problem auftritt dieses nachverfolgen zu können. Jedoch kann es vorkommen, dass eine andere Organisation diese Logdaten anfordert um Informationen über einen bestimmten Benutzer oder eine Benutzergruppe erlangen zu können. Dazu muss die Organisation, die die Daten anfordert in irgendeiner Form über mehr

Macht verfügen. Dies ist zum Beispiel bei Regierungen, auch anderer Länder, der Fall.

In diesen beiden und vielen anderen Fällen kann eine Implementierung eines *private information retrieval* die Benutzer schützen.

3 Funktionsweise

4 Möglichkeiten einer Untergrabung

5 Implementation