DQ0
Offener Datenzugang bei bestem Datenschutz

AF INSTITUTE



shutterstock

Mit DQ0 kann ein Dateneigentümer hochsensible digitale Informationen in einer sicheren Enklave speichern und Dritten unter Wahrung des Datenschutzes vollen Zugriff gewähren. Die Daten bleiben beim Eigentümer.
Das robuste Sicherheitskonzept der DQ0 Zugriffs-Software (Datenschutz, Organisation/ Prozesse und technische Implementierung) wurde vom TÜV geprüft und zertifiziert.

Beispiel öffentliche Gesundheit

Krankenhäuser und Gesundheitsbehörden können mit DQ0 Patientendaten, Diagnosen, Therapien und Krankheitsverläufe zentral in der Enklave speichern. Außenstehende Wissenschaftler und Fachärzte können die Daten auswerten und Erkenntnisse daraus gewinnen. Sie haben quasi vollen Zugriff auf für sie wichtige Informationen. Was sie jedoch nicht sehen, sind schützenswerte Daten wie z.B. der Name oder die Adresse der Patienten.

Anwendung in der Forschung

Ein typischer Anwendungsfall wäre die Weitergabe großer Datenbestände an außenstehende Forscher. Sie können künstliche Intelligenz auf die Daten anwenden und damit z.B. Modellrechnungen erstellen und neue Erkenntnisse für die Wissenschaft gewinnen.
Da alle Informationen, die dem Datenschutz unterliegen, nicht mehr sichtbar sind, können

die Daten ohne Bedenken für Dritte geöffnet werden.

Einzigartige Vorteile

- Mit DQ0 bleibt der Datenbestand unverändert. Nichts wird geschwärzt, anonymisiert, synthetisiert oder pseudonymisiert. Die Daten bleiben zur Gänze vorhanden. Auch muss niemand mit der Anonymisierung oder Pseudonymisierung oder mit ähnlichen Verfahren beauftragt werden.
- Modellrechnungen auf Basis dieser Daten haben – weil die Daten nicht verändert wurden – eine höhere Qualität.
- Anwender bekommen zwar Zugang zu Daten hoher Güte, aber nicht zu jenen Informationen, die dem Datenschutz unterliegen.

Standardsysteme schützen nicht ausreichend

Generell steht der Datenschutz bei Datenabfragen vor einer zentralen Frage: Wie kann im Zuge einer Datenabfrage die Qualität der Antwort möglichst hoch und gleichzeitig der Abfluss von schützenswerten Informationen aus den Daten möglichst gering gehalten werden?

Beliebte Methoden, um sensible Daten Dritten für wissenschaftliche Zwecke zur Verfügung zu stellen, sind Anonymisierung, Pseudonymisierung oder Synthetisierung. Bei diesen Ansätzen sinkt die Analysequalität und die Daten werden verändert, um die Informationen zu schützen.

Hinzu kommt: **Zahlreiche Studien und Fälle haben gezeigt, dass diese Maßnahmen die privaten Informationen nicht ausreichend schützen.**

Fortschrittlichster Ansatz

Die DQ0 Datenquarantäne arbeitet dagegen nach der wissenschaftlich fortschrittlichsten Methode, der Differential Privacy. **Die Quarantäne schließt die Daten sicher ein und erlaubt eine Analyse, ohne die Daten selbst zu manipulieren.** Lediglich die Antwort zu Datenabfragen wird so verändert, dass die Informationen in den Daten geschützt sind. Die Modelle werden bei den Daten trainiert und nur geprüfte, allgemeingültige Informationen verlassen die Datenquarantäne; so **sind zu keinem Zeitpunkt Rückschlüsse auf einzelne Personen oder geheime Einzelinformationen möglich.**

Kombination mit dem AFI Anonymizer

Der AFI Anonymizer kann innerhalb der DQ0 Plattform angewendet werden.

Somit sind die Eingangsdaten optimal durch DQ0 geschützt, und der Dateneigentümer kann die durch den AFI Anonymizer anonymisierten oder pseudonymisierten Daten nach Prüfung zur öffentlichen Verwendung freigeben.

Lokal oder remote

Anwender können mit DQ0 lokal oder remote arbeiten. Für den lokalen Modus muss das SDK installiert werden.

Damit können Anwendungen für maschinelles Lernen verfasst werden, die dann in der Enklave sicher verarbeitet werden. Für den Remote-Modus muss sich der Nutzer mit der Proxy verbinden.

Die Software wird ohne Daten ausgeliefert, die Entwicklung erfolgte mit anwendungstypischen Testdaten.

www.af-institute.at

© 2021 AF Private Institute for Research and Ethical Use of Artificial Intelligence GmbH.
Grünbergstraße 15, Stiege 2, Top 1.2a, A-1120 Vienna, Austria. All rights reserved.