Zusammenfassung

Vernetzte Fahrzeuge erzeugen kontinuierlich große Mengen sensibler Sensordaten, die für Mobilitätsdienste, Versicherer und Anwendungen von Drittanbietern wertvoll sind. Die Weitergabe dieser Daten ist jedoch mit Sicherheits- und Datenschutzrisiken verbunden. Dazu zählen die unbefugte Verfolgung von Fahrerinnen und Fahrern, die langfristige Profilbildung des Fahrverhaltens, die Ableitung sensibler Merkmale sowie der Missbrauch oder die Offenlegung personenbezogener Daten durch Dritte. Diese Risiken müssen im Einklang mit Datenschutzvorschriften wie der DSGVO gemindert werden. Diese Dissertation begegnet diesen Herausforderungen, indem sie ein datenschutzorientiertes Data-Governance-Rahmenwerk für vernetzte Fahrzeuge vorschlägt, das die fahrzeuginterne Zugriffskontrolle, den organisationsübergreifenden Datenaustausch und datenschutzfreundliche Datenanalysen umfasst.

Erstens werden auf der Zugriffskontrollschicht fahrzeugspezifische Anforderungen identifiziert, nämlich zeitbasierte, ortsbasierte und frequenzbasierte Datenzugriffe, und ein erweitertes XACML-basiertes Modell namens XACML4M (XACML for Mobility) vorgeschlagen. XACML4M führt Komponenten wie die Vehicle Data Environment, Time Extension, Geolocation und Polling Frequency Providers ein, um eine fein-granulare, dynamische und kontextabhängige Zugriffskontrolle zu ermöglichen. Ein funktionaler Prototyp wurde auf einem Raspberry Pi 4 implementiert und anhand realer Use-Case-Policies validiert, was die praktische Umsetzbarkeit dynamischer Autorisierung in Fahrzeugumgebungen bestätigt.

Zweitens stellt die Dissertation für den organisationsübergreifenden Datenaustausch Sticky-PRE (Sticky-Proxy Re-Encryption) vor, ein Protokoll, das maschinenlesbare Sticky Policies mit Proxy Re-Encryption kombiniert. Sticky-PRE stellt sicher, dass nutzerdefinierte Zugriffsbedingungen über den gesamten Datenlebenszyklus hinweg, auch über Organisationsgrenzen hinaus, erhalten bleiben, wobei gleichzeitig Vertraulichkeit, Integrität und Verantwortlichkeit der Daten gewahrt werden. Das Protokoll wurde unter einem honest-but-curious-Bedrohungsmodell analysiert und quantitativ anhand von Leistungsbenchmarks für Verschlüsselung, Re-Verschlüsselung und Entschlüsselung bewertet, was seine sichere und effiziente Eignung für Kontexte vernetzter Fahrzeuge belegt.

Drittens untersucht die Arbeit für nachgelagerte Datenanalysen das Spannungsfeld zwischen Datenschutz und Nutzbarkeit in der Kfz-Versicherungsanalyse unter Verwendung realer anonymisierter Daten. Die Studie bewertet systematisch, wie Anonymisierungstechniken, k-Anonymität und l-Diversität (Distinct-, Shannon-Entropy- und rekursive (c,l)-Diversität) die Leistung von Machine-Learning-Modellen zur Vorhersage von Versicherungsansprüchen beeinflussen. Die Ergebnisse zeigen, dass sich das Re-Identifikationsrisiko deutlich verringern lässt, während gleichzeitig eine wettbewerbsfähige Vorhersageleistung erhalten bleibt. So erreicht beispielsweise eine Konfiguration auf Basis von Distinct l-Diversität mit l=10 in Kombination mit einem Support-Vector-Classifier ein Restrisiko von 0.049% und ein k-Anonymitätsniveau von 2013 bei nur geringfügigen Einbußen in der Vorhersagegenauigkeit im Vergleich zum ursprünglichen Datensatz. Diese Ergebnisse bieten praktische Hinweise darauf, wie Organisationen Anonymisierungsparameter wählen können, die Datenschutz und analytischen Nutzen ausbalancieren. In ihrer Gesamtheit realisieren diese miteinander verknüpften Beiträge ein umfassendes Rahmenwerk für eine sichere, nachvollziehbare und datenschutzfreundliche

Weitergabe von Fahrzeugdaten, das mit modernen Datenschutzprinzipien im Einklang steht und gleichzeitig aussagekräftige datengetriebene Dienste ermöglicht.