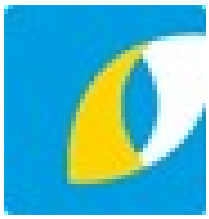

**Erkennung von Inferenzangriffen mit Sensordaten**

Die Erfassung personenbezogener Daten bei sozialen Interaktionen ist für Unternehmen immer wichtiger geworden. Dennoch müssen die Organisationen gemäß der DSGVO (Datenschutz-Grundverordnung) die gesammelten Daten schützen. Zugriffskontrollmechanismen (*Access Control*, AC) werden traditionell eingesetzt, um Informationssysteme vor unberechtigtem Zugriff auf sensible Daten zu schützen. Die zunehmende Verfügbarkeit von persönlichen Sensordaten dank des *Internet of Things* (IoT) orientierter Anwendungen motiviert neue Dienste Erkenntnisse über Einzelpersonen zu sammeln und zu bieten. Folglich wurden Data-Mining-Algorithmen vorgeschlagen, um aus gesammelten Sensordaten persönliche Erkenntnisse abzuleiten. Obwohl diese generell für nicht bösartige Zwecke verwendet werden, können Angreifer diese Ergebnisse für sich ausnutzen. So können diese Erkenntnisse mit anderen Datentypen kombinieren werden, um auf neue sensible Informationen zu schließen. Dadurch wird die Privatsphäre von Personen weiter verletzt. Die Umgehung von AC-Mechanismen dank solcher Erkenntnisse ist daher ein konkretes Problem.

Wir schlagen ein System zur Erkennung von Schlussfolgerungen vor, das auf der Analyse von Abfragen an eine Sensordatenbank basiert. Das durch diese Abfragen gewonnene Wissen und die Inferenzkanäle, die dem Einsatz von Data-Mining-Algorithmen auf Sensordaten zur Ableitung individueller Informationen entsprechen, werden mit Hilfe des “*Raw sensor data based Inference ChannEl Model*” (RICE-M) beschrieben. Die Erkennung erfolgt durch ein auf “*RICE-M based inference detection System*” (RICE-Sy). RICE-Sy berücksichtigt zum Zeitpunkt der Abfrage das Wissen, welches ein Benutzer über eine neue Abfrage und über seine Abfragehistorie erlangt hat, und bestimmt, ob dieses Wissen ausreicht, um dem Benutzer zu erlauben, einen Kanal zu betreiben. Auf diese Weise können Systeme zum Schutz der Privatsphäre die von RICE-Sy ermittelten Rückschlüsse nutzen und die von den Angreifern über eine Sensordatenbank erhaltenen Informationen über einzelne Personen berücksichtigen, um diese Personen weiter zu schützen.