Universität Bayreuth
Professuren Wirtschaftsinformatik
Prof. Dr. Eymann,
Prof. Dr. Röglinger,
Prof. Dr. Strüker

Ansprechpartner
Johannes Sedlmeir

Telefon
+49 157 51618033

E-Mail
johannes.sedlmeir@fim-rc.de

Bachelorarbeit / Masterarbeit

Business Applications of Privacy Enhancing Technologies

In den vergangenen Jahren gab es rasante Fortschritte in der Praktikabilität von Technologien, die die Korrektheit oder Compliance von Berechnungen transparent zeigen, ohne die Vertraulichkeit der zugrundeliegenden Daten aufgeben zu müssen. Das wohl am besten bekannte und aktuell am stärksten im Fokus stehende Beispiel hierfür sind sogenannte Zero-Knowledge Proofs. Aktuell werden Zero-Knowledge Proofs vor allem im Kontext von Kryptowährungen bzw. Blockchain-Technologie eingesetzt. Dadurch kann die beiden in diesem Kontext wohl größten Probleme, die beide durch die redundante Datenhaltung und Berechnung von Prozessen auf Blockchains bedingt sind: Datenschutz und Skalierbarkeit. Durch den Hype um Kryptowährungen und die entsprechenden ökonomischen Anreize, die Probleme dieser Kryptowährungen innovativ zu lösen, sind Zero-Knowledge Proofs und verwandte Technologien, die Berechnungen auf versteckten oder verschlüsselten Daten ermöglichen, in den vergangenen Jahren deutlich praktikabler geworden. Zu nennen sind hier ebenfalls Secure Multiparty Computation (diese wird etwa bei so-genannten Trusted Setup Zeremonien für Zero-Knowledge Proofs benötigt) oder Fully Homomorphic Encryption (eine Verschlüsselungsmethode, die etwa das Trainieren oder Auswerten von Machine Learning Algorithmen auf verschlüsselten Daten ermöglichen kann). Diese unterscheiden sich nach wie vor wesentlich hinsichtlich ihrer Komplexität und Technologiereife, aber die erheblichen Fortschritte der letzten Jahre legen nahe, dass in naher Zukunft zahlreiche praktische Anwendungen zu erwarten sind. Ein Beispiel hierfür könnte etwa folgendes Problem sein: Ein Unternehmen möchte Produkte mit bestimmten Eigenschaften bestellen und müsste hierzu einen „Ka-talog“ eines Anbieters durchsuchen, um den besten Fit zu erzielen. Möglicherweise möchte aber der Anbieter nicht seine komplette Produktpalette offenlegen. Auf der anderen Seite möchte das Unternehmen seine Suchanfrage gegenüber dem Anbieter nicht offenlegen, da dieser sonst ggf. sein Angebot oder Preise noch abändern könnte. Mit Technologien des Privacy Preserving Computing könnte ein solches „Matching“ von Angeboten und Anfrage geschehen, ohne dass der Anbieter seinen Katalog und das Unternehmen seine Anfrage gegenseitig (und auch gegenüber irgendeiner Drittpartei) offenlegen müsste.

Ziel der Arbeit ist eine Analyse verschiedener Technologien, die dem Umfeld der Privacy Enhancing Technologies zuzuordnen sind, und/oder Einsatzmöglichkeiten in Unternehmen bzw. der öffentlichen Verwaltung. Ein Grundinteresse an angewandter Kryptographie ist hierbei nötig; jedoch kann das Thema gut ohne Vorwissen auf diesem Gebiet bearbeitet werden, da die Protokolle und deren Eigenschaften nur auf einer oberflächlichen Basis verstanden werden müssen.

Empfohlene Einstiegsliteratur: Nach Rücksprache mit dem Betreuer.

Betreuer: Sedlmeir, Johannes, M.Sc.