

Halle (Saale), 28.10.2021

Medieninformation

Weiteres Projekt der Cyberagentur gestartet – „Encrypted Computing“ als vertrauliche und datenschutzkonforme Technologie

Eine sichere Verschlüsselung von Daten ist eine Voraussetzung in nahezu allen Bereichen der Informationsverarbeitung. Das gilt sowohl für den Datenverkehr im Alltag jedes Einzelnen als auch für besonders sicherheitssensible Bereiche wie Polizei, Nachrichtendienste oder Militär.

Darüber hinaus wird die sichere Analyse, Bearbeitung und Übermittlung von Daten mit Blick auf die technologischen Trends für die Zukunft wichtiger, sowohl für gesellschaftliche als auch für sicherheitsrelevante Behörden. Heutige kryptographische Verfahren erlauben es, Daten lediglich bei ihrer Übertragung und ihrer Speicherung geheim zu halten. Die Wahrung der Geheimhaltung von Daten während einer Verarbeitung ist aktuell nicht möglich.

Welche Verfahren erlauben es praktikabel, sensible und/oder sicherheitsrelevante Daten zu analysieren und zu bearbeiten, ohne sie entschlüsseln zu müssen? Das ist die zentrale Frage des nächsten Projekts der Cyberagentur, welches nun ausgeschrieben wurde.

„Dieses Rechnen mit verschlüsselten Daten, das sogenannte ‚Encrypted Computing‘, birgt ein enormes Innovationspotenzial. Besonders vielversprechend erscheint dabei die sogenannte vollständige homomorphe Verschlüsselung (FHE)“, sagt Michael John, der Themenverantwortliche für den Bereich „Encrypted Computing“ bei der Cyberagentur.

Beispielsweise ermöglicht diese Technologie eine Verarbeitung von Daten in Cloudumgebungen, ohne dass der Cloud-Provider als Drittpartei in der Lage wäre diese Daten einzusehen.

Ein weiteres potenzielles Anwendungsszenario könnte die Nutzung von verschlüsselten Trainings- und Anwendungsdaten für das Maschinelle Lernen sein. „Encrypted Computing“ würde es erlauben, verschlüsselte Daten (Bild, Text, Video, Sprache) durch Künstliche Intelligenz auswerten zu lassen, ohne dass das System Kenntnis über den Inhalt erlangen kann. Dies könnte dann u.a. die KI-gestützte Videoüberwachung erlauben, ohne dass der Inhalt der Videodaten dargelegt werden müsste. In einem weiteren Schritt könnte auch das

Anlernen der Künstlichen Intelligenz auf verschlüsselten Daten durchgeführt werden. Dies wäre insbesondere von Interesse, wenn die Daten sehr sensibler Natur sind. „Encrypted Computing“ würde es so ermöglichen, Forscher:innen Trainingsdaten bereitzustellen, die sonst nicht weitergegeben werden könnten.

Während die prinzipielle Machbarkeit dieser kryptografischen Techniken weitgehend geklärt ist, sind noch viele Fragen insbesondere zur Effizienz und Konkurrenzfähigkeit der Verfahren ungeklärt. Zur Vorbereitung eines Forschungswettbewerbs zu „Encrypted Computing“ führt die Cyberagentur nun zunächst ein Projekt zu den verschiedenen zugrundeliegenden Technologien durch. Ziel des Projekts ist die Schaffung eines Rahmenwerks mit Ontologie, Kategorisierung der Einsatzmöglichkeiten, Bewertung von Leistungsfähigkeit und Sicherheit sowie der anwendungsbezogene Vergleich der Verfahren.

Die Frist für die Einreichung der Skizzen läuft bis zum 22. November 2021. Mitmachen könnten Hochschulen und außeruniversitäre Forschungseinrichtungen, Unternehmen und Start-ups.

Alle weiteren Informationen finden Sie auf unsere [Website](#).

Hintergrund Cyberagentur:

Die Agentur für Innovation in der Cybersicherheit, kurz Cyberagentur, wurde im Sommer 2020 in der Rechtsform einer Gesellschaft mit beschränkter Haftung gegründet. Einzige Gesellschafterin ist die Bundesrepublik Deutschland, gemeinsam vertreten durch das Bundesinnenministerium und das Bundesverteidigungsministerium. Sie versteht sich als treibende Kraft einer offenen Innovations- und Wagniskultur sowie für ein lebendiges Ökosystem zur Förderung von Cybersicherheitstechnologien. Die Cyberagentur will Forschung sowie bahnbrechende Innovationen im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien im Bereich der inneren und äußeren Sicherheit vorantreiben. Mit diesem Auftrag leistet sie einen Beitrag zur technologischen Souveränität Deutschlands im Cyber- und Informationsraum. Die Cyberagentur forscht nicht selbst. Aktuell arbeiten rund 25 Beschäftigte bei der Cyberagentur, mit einem Ausbauziel von etwa 100 Beschäftigten. Ihr Sitz ist in Halle (Saale).

Kontakt Team Kommunikation:

Verena Frank, +49 151 44150645, <frank@cyberagentur.de>