Fraunhofer FIT

Fraunhofer-Institut für Angewandte Informationstechnik FIT

Datenschutz und Vertraulichkeit im Zeitalter von zuverlässiger Big Data

Lösungen für Datenschutz und Datensouveränität

Die Verlagerung hin zu Big Data und KI-gesteuerter Datenverarbeitung eröffneten unvorhergesehene Potenziale, führten aber auch zu vielfältigen neuen Herausforderungen bezüglich der Kontrolle über diese Daten und der daraus gewonnenen Erkenntnisse. Die Forschungsgruppe Datenschutz und Datensouveränität befasst sich hierbei mit der Erforschung praktischer, die Privatsphäre steigernder Technologien (PETs) im Zeitalter von KI und zuverlässiger Big Data.

Gruppenüberblick

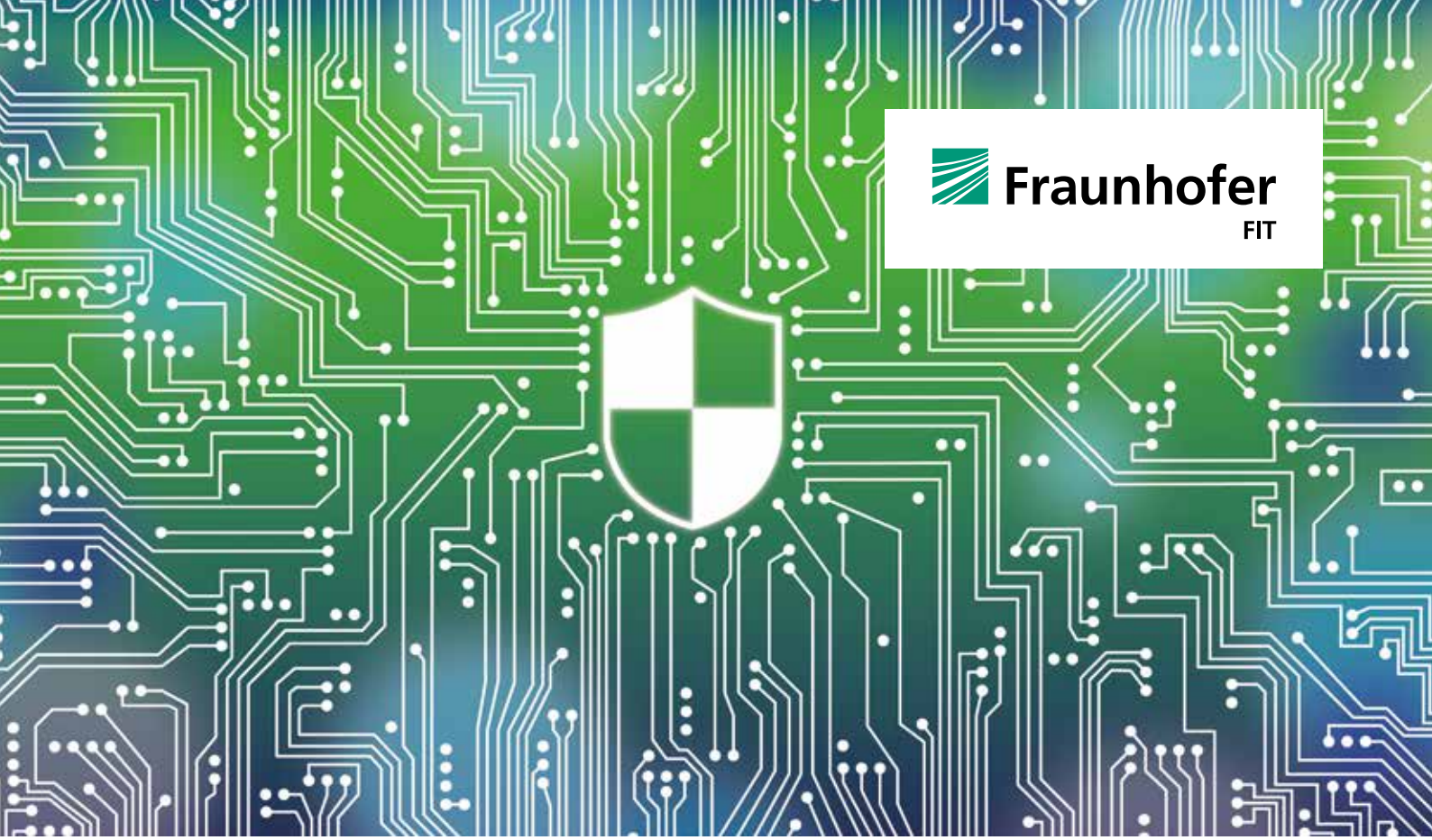
Die Forschungsgruppe Datenschutz und Datensouveränität (DPS) ist von dem Wunsch angetrieben, latente Potenziale des Teilens von Daten zu entfalten, indem sichergestellt wird, dass der Dateninhaber die Kontrolle behält und die Vorteile und auch Folgen einer gesteigerten Offenheit in Hinblick auf Daten bewerten kann. Wir streben an, die Extraktion von Wissen und die Ableitung von Erkenntnissen daraus sicher und einfach zu gestalten, insbesondere angesichts der Anforderungen durch Verordnungen wie die DSGVO oder die NIS-2-Richtlinie.

Forschungsschwerpunkt

Die Forschung der Gruppe konzentriert sich auf die technischen Aspekte der Privatsphäre und Vertraulichkeit sowie die Anwendung von KI und insbesondere Large Language Models (LLMs) im Kontext von IT-Sicherheit und Datenschutz. Als solche sind wir an den technischen Garantien interessiert, die von PETs und deren Anwendung in modernen Datenplattformen von Cloud-Anwendungen über Datenräume bis hin zu Blockchains hergestellt werden können. Das Zusammenspiel von KI-Technologien und PETs ist für uns von besonderem Interesse.

Kollaborationen mit der Industrie

Wir sind bestrebt, Unternehmen mit unserer Erfahrung dort zu unterstützen, wo sie bestmöglich weiterhilft, insbesondere in Form von FuE-Aufträgen sowie Beratungs- oder Weiterbildungsdienstleistungen in den Bereichen Datenschutz, KI und PETs. Wir erweitern unser Know-how kontinuierlich durch national und international geförderte gemeinsame Forschungsprojekte mit Industriepartnern, z.B. gefördert durch das BMBF oder die EU HORIZON-Programme.



Fraunhofer FIT

Unser Hauptprodukt: Datenaustausch für Cybersecurity-Playbooks

Eines der eindrucksvollsten Beispiele für die Umsetzung unserer Vision ist unser Ansatz für das Management von teilbaren Cybersecurity-Playbooks (SASP). Cybersecurity-Playbooks stellen den de-facto-Standard für die Dokumentation von Prozessen zur Reaktion auf Cybersicherheitsvorfälle dar. Diese Playbooks werden jedoch üblicherweise nur innerhalb einer Organisation gepflegt, was zu unstrukturierten, unvollständigen, veralteten und organisationsübergreifend redundant verwalteten Dokumentationen führt. Vor allem angesichts der NIS-2-Richtlinie und der Anforderungen an eine standardisierte Berichterstattung über Sicherheitsvorfälle ist dieser Status Quo zunehmend problematisch.

Über das Teilen von Cybersecurity-Playbooks

Um diese Beschränkungen zu überwinden, entwickeln und erweitern wir SASP als Management-Plattform für den Übergang von un- oder semistrukturierten Playbooks zu standardisierten, maschinenlesbaren und feinschrittigen Beschreibungen von Cybersicherheits-Playbooks. SASP basiert auf dem CACAO-Standard für die digitale Spezifikation von Cybersicherheits-Playbooks. Auf der Grundlage des CACAO-Standards sorgt SASP dafür, dass Organisationen ein breitflächiges gemeinsames Verständnis für die Interpretation von Cybersecurity-Playbooks aufbauen können. Darüber hinaus bietet SASP den Schutz der Vertraulichkeit sensibler Daten, eine nutzerfreundliche Bedienung und eine Visualisierung von Playbooks basierend auf Praktiken aus der Geschäftsprozessmodellierung.

Nächste Schritte zur verbesserten Anwendbarkeit

Derzeit erweitern wir unser SASP-Framework, um die Nutzerfreundlichkeit weiter zu steigern. Insbesondere entwickeln wir eine LLM-Integration, mit der ältere Playbooks in entsprechende CACAO-Playbooks, die dann über SASP verwaltet werden, überführt werden. Darüber hinaus erforschen wir, wie aus diesen maschinenlesbaren Playbooks wieder an verschiedene Kontexte angepasste Playbooks in natürlicher Sprache generiert werden können, beispielsweise zur Berücksichtigung der technischen Kenntnisse unterschiedlicher Nutzergruppen.

Kontakt

Dr. Avikarsha Mandal
Gruppenleitung
Datenschutz und Datensouveränität
Telefon +49 241 80-21510
avikarsha.mandal@fit.fraunhofer.de

Dr. Roman Matzutt
Stellvertretende Gruppenleitung
Datenschutz und Datensouveränität
Telefon +49 241 80-21541
roman.matzutt@fit.fraunhofer.de

Abteilung
Data Science und Künstliche Intelligenz

Fraunhofer Institut für
Angewandte Informationstechnik FIT
Ahornstraße 55
52074 Aachen | Germany
www.fit.fraunhofer.de