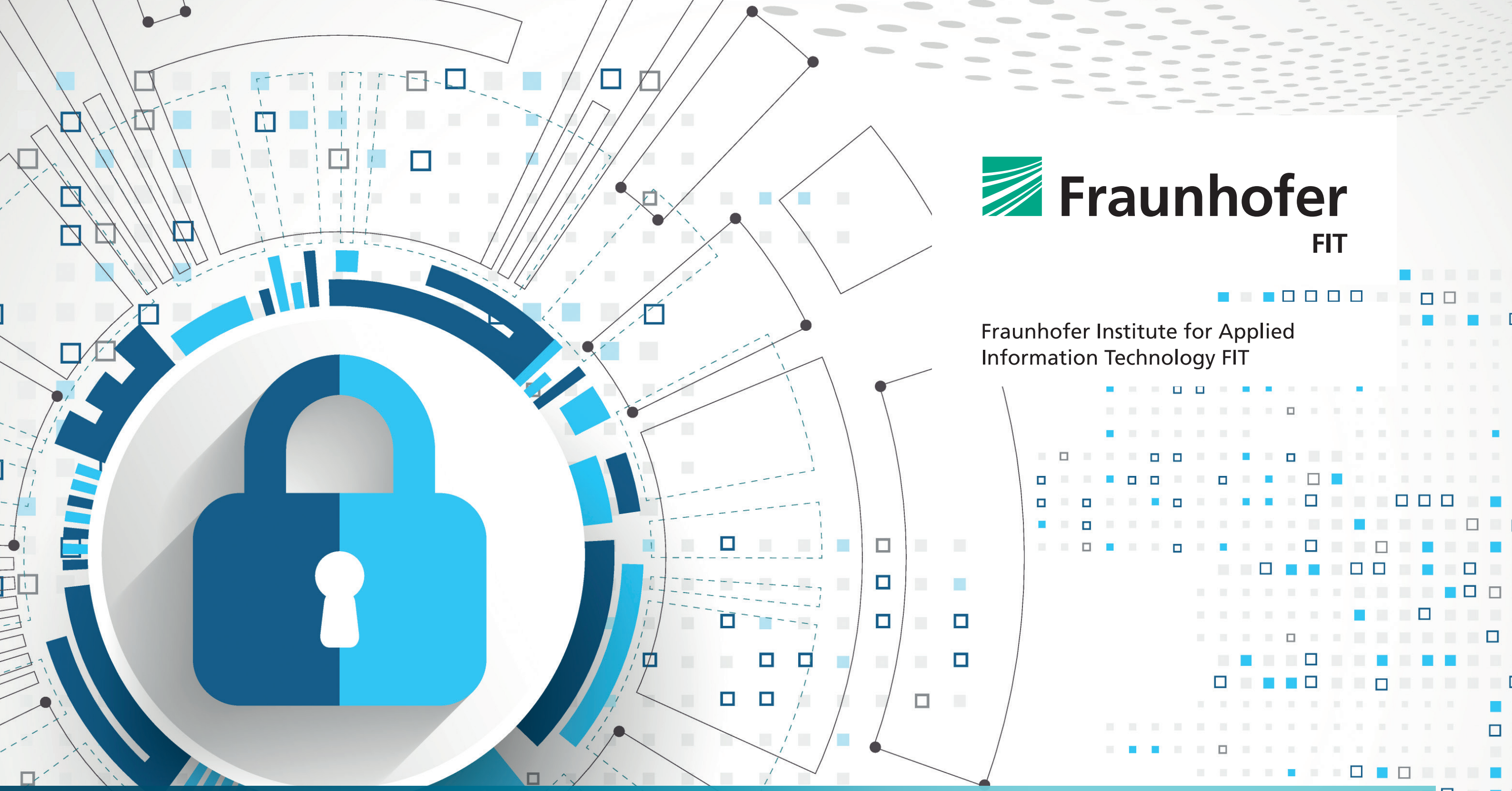


Fraunhofer
FIT

Fraunhofer Institute for Applied
Information Technology FIT

Privacy and Confidentiality in the Age of Dependable Big Data

Data Protection and Sovereignty Solutions

The shift toward Big Data and AI-driven data processing opened up unforeseen potentials, but also introduced new, manifold challenges to keep control over that data and insights gained from it. Our vision for modern *Data Protection and Sovereignty* thus entails the research and development of practical Privacy-Enhancing Technologies (PETs) in the age of AI and dependable Big Data.

Core Competencies

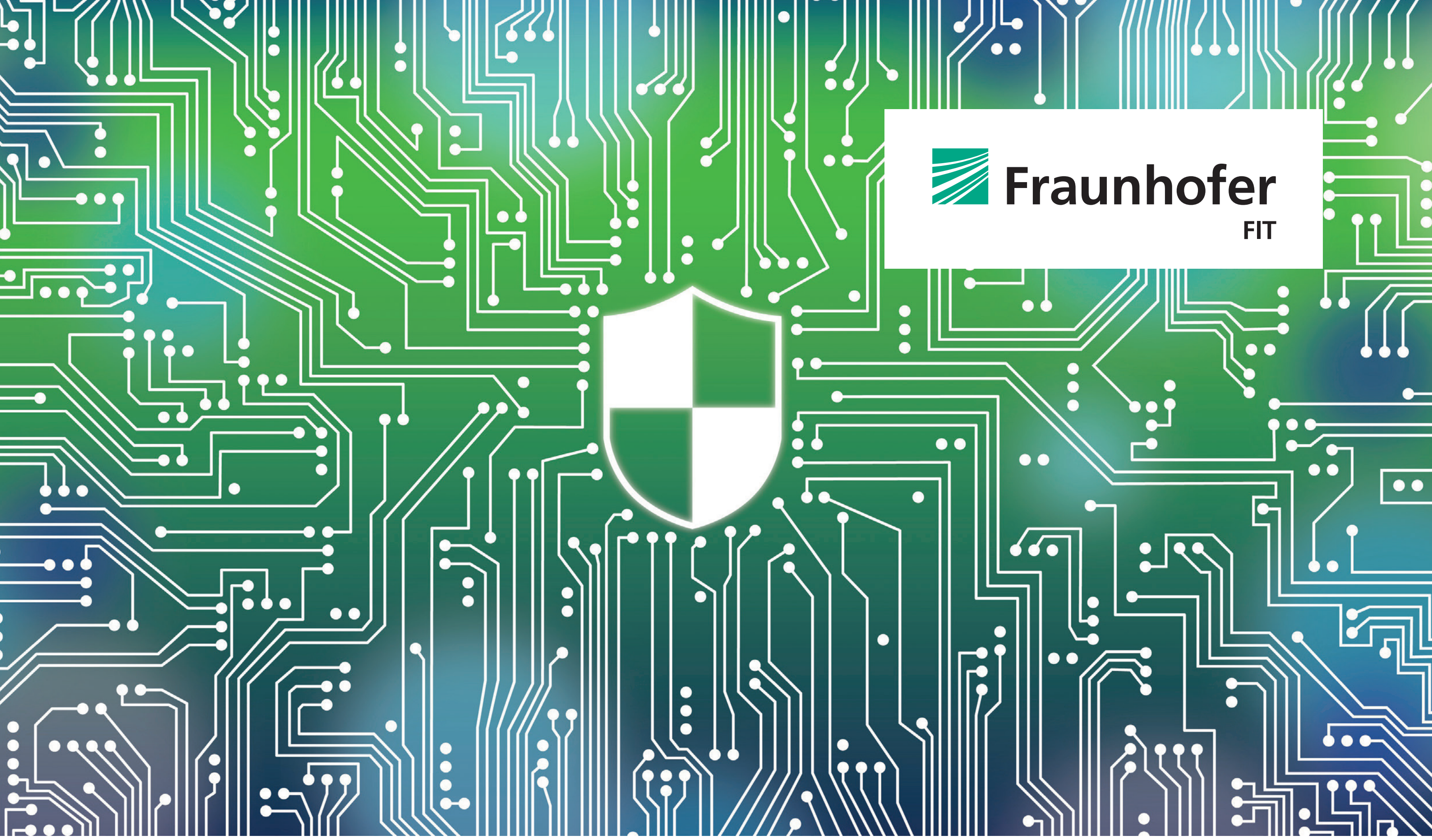
As the Data Protection and Sovereignty Group, our core competencies lie in our commitment to unlocking the latent potential of data sharing while safeguarding the control of data owners. Our small yet ambitious research team is dedicated to enabling individuals to assess both the benefits and consequences of increased data openness. We excel in ensuring secure and user-friendly processes for knowledge extraction and insight derivation, specifically due to requirements prompted by regulatory frameworks such as GDPR and NIS 2 Directive.

Research and Development Endeavors

The research of the DPS group focuses on the technical aspects of privacy and confidentiality as well as the application of AI and particularly Large Language Models (LLMs) to problems from the domain of security and privacy. As such, we are interested in the technical guarantees that can be provided by PETs and their application in modern data-sharing applications, ranging from cloud applications over data spaces to distributed ledgers, i.e., blockchains. The interplay of AI technologies and PETs is of particular interest to the DPS group.

Industry Solutions

We continuously expand our expertise to support our industrial partners. For instance, we engage in extensive R&D activities to help companies manage their increasingly indispensable cybersecurity playbooks. Further, we offer consultation services and customized training focused on PETs to enhance proficiency in this vital area.



Our Main Product: Sharable Cybersecurity Playbooks

Remain one step ahead of cybercriminals with our management tool for sharable cybersecurity playbooks! Cybersecurity playbooks constitute the de facto standard of documenting processes for responding to cybersecurity incidents. However, these playbooks are routinely maintained within the confinements of a single organization, which leads to redundantly managed, unstructured, incomplete, or outdated documentation. Especially in the face of the NIS 2 Directive and its upcoming requirements for standardized cyber incident reporting, this current state is becoming increasingly troublesome.

On Sharing Cybersecurity Playbooks

To overcome these limitations, we develop and extend our Semantic Web-based Approach for the Management of Sharable Cybersecurity Playbooks (SASP) as a management platform for transitioning from unstructured and semi-structured documentation to standardized, machine-readable, and fine-granular descriptions of cybersecurity playbooks. SASP relies on the CACAO standard for digitally specifying cybersecurity playbooks. Building upon the foundation provided by CACAO, SASP ensures that organizations can establish a common understanding to foster the interpretability of playbooks across the board. Additionally, SASP protects confidentiality of sensitive data, usability, and visualization of playbooks based on practices from business process modelling.

What's Next?

We are extending our SASP framework by adding LLM support to read legacy cybersecurity playbooks and derive corresponding CACAO rules to be managed via SASP. Further, we are exploring methods to generate human-readable process descriptions from those CACAO rules, e.g., for allowing dynamic adjustments tailored to different user skill levels.

Contact

Dr. Avikarsha Mandal
Group Lead
Data Protection and Sovereignty Solutions
Phone +49 241 80-21510
avikarsha.mandal@fit.fraunhofer.de

Dr. Roman Matzutt
Deputy Group Lead
Data Protection and Sovereignty Solutions
Phone +49 241 80-21541
roman.matzutt@fit.fraunhofer.de

Department
Data Science and Artificial Intelligence

Fraunhofer Institute for
Applied Information Technology FIT
Ahornstraße 55
52074 Aachen | Germany
www.fit.fraunhofer.de