CyLab PARTNER SUCCESS STORY

SIEMENS

ABOUT SIEMENS

Siemens is a multinational company headquartered in Munich, Germany focusing on industry, energy, and healthcare products and services.

SIEMENS' MAIN PRODUCTS

- Power generation technologies
- Industrial and buildings automation
- Medical technologies

SIEMENS' CHALLENGE

Utilizing customer data to optimize Siemens' products and services while preserving customers' privacy.

> "Privacy-preserving analytics is a topic with significant importance for Siemens."

– Martin Otto, Head of Research Group
Cybersecurity Service Innovation, Siemens

BACKGROUND ON SIEMENS' DATA PRIVACY CHALLENGE

Digitalization, i.e., generating value-add from data, is showing tremendous potential for benefits for industrial applications. For example, designing and optimizing intrusion detection systems to protect customers' computer networks and control systems require data logs and network traffic data, but this data may contain sensitive information that customers are not willing to share.

Data owners need to know that direct access is secure, and required limitations on acceptable use are adhered to for shared data. This goes beyond customers' legitimate desire to protect their intellectual property and trade secrets. It also includes regulatory requirements, such as those for data privacy. While security precautions to protect access to data are available, methods that would allow using methods to provide provable anonymization and privacy would make data analytics on sensitive data much easier.

CyLab Carnegie Mellon University
Security and Privacy Institute

DoppelGANger: A TOOL TO MEET SIEMENS' CHALLENGE

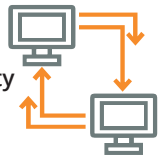
DoppelGANger is a tool developed by CyLab researchers that utilizes generative adversarial networks, or GANs, which employ machine learning techniques to synthesize datasets that have the similar characteristics as the original "training" dataset but have been stripped of the sensitive information.

Most data modelling tools require extensive knowledge in mathematical modeling, which creates a barrier for data sharing across different levels of expertise. DoppelGANger, however, requires little to no prior knowledge of the dataset and its configurations due to the fact that GANs themselves are able to generalize across different datasets and use cases. This makes DoppelGANger highly flexible, and that flexibility is key to data sharing in various cybersecurity situations.

CYLAB LEAD RESEARCHER
Giulia Fanti, Assistant Professor, Department of Electrical and Computer Engineering

> **DoppelGANger provides a novel approach to generate synthetic data that is close enough to actual data to enable meaningful data analytics while preserving privacy."**
>
> –Giulia Fanti, Assistant Professor, Department of Electrical and Computer Engineering

> **DoppelGANger is a promising approach for sharing data between customers and Siemens."**
>
> –Martin Otto, Head of Research Group-Cybersecurity Service Innovation, Siemens



IMPACT OF THE CYLAB-SIEMENS PARTNERSHIP

- With Siemens' support, Prof. Fanti and her team have published four papers - three at top venues, and one that was a finalist for a Best Paper Award - towards improving DoppelGANger's fidelity, privacy, and interpretability.
- Siemens gained the transfer of knowledge about the state of the art, current challenges, and possibilities of technology and solutions to allow them to evaluate whether they should or should not focus on such technology.

For assistance in designing the collaborative engagement that best fits your needs, please contact us at: partnerships@cylab.cmu.edu

> **These intermediate results have both influenced our internal research agenda, as well as resulted in strategic decisions about capability roadmaps. We remain impressed about the expertise and innovation power of CyLab's research community, and appreciate the opportunities that we are being provided to access researchers, discuss ideas, and gain insights into current and novel research topics and results."**
>
> –Martin Otto, Head of Research Group-Cybersecurity Service Innovation, Siemens

Carnegie Mellon University
Security and Privacy Institute
CyLab

www.cylab.cmu.edu