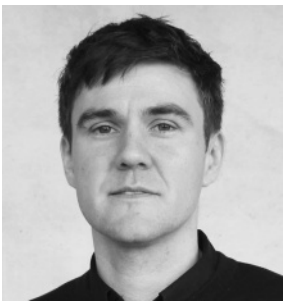
Agnes Koschmider
Christian-Albrechts-Universität zu Kiel
ak@informatik.uni-kiel.de

Martin Degeling
Ruhr-Universität Bochum



Matthias Weidlich
Humboldt-Universität zu Berlin

Process Analytics over IoT-based Event Streams with Privacy Guarantees

Every day large amounts of event streams are created in the Internet of Things (IoT). A lot of these events include or refer to personal data, which need to be protected. Awareness of privacy issues in IoT-based event streams has risen, particularly since the General Data Protection Regulation (GDPR) was put into force. Among other things, it requires organizations to consider privacy throughout the whole data lifecycle, from collection and processing to deletion. Systems that exploit IoT-based event streams, however, require fundamentally new practices for privacy-by-design or privacy-by-architecture development that are different from those for conventional information systems in terms of user-centered access control and identity management. In the past, the focus of privacy considerations in system design was often on the protection of data that directly relate to a person, i.e. salary, email address, or customer number. With IoT-based event streams, privacy-aware system design faces plenty of new challenges. Such streams continuously produce an infinite number of heterogonous events that are highly dependent on each other and can occur concurrently, alternatively, or independently. Stream processing systems aim to identify meaningful knowledge and process-related information from event streams in real-time, thereby creating threats to personal privacy. This calls for techniques for data analytics over IoT-based event streams with provable data protection through privacy guarantees.

Analytics in terms of process mining enables valuable insights into the compliance and performance of process execution using IoT-based event streams. However, process mining over IoT event data can also uncover plenty of personal activities and behavior patterns that require protection. Even process mining over encrypted event data might uncover sensitive information. Moreover, privacy requirements have to be chosen in relation to the threat the data pose and are, therefore, situation and application specific. Eventually, it will, therefore, be necessary to provide models and methods to balance privacy requirements and analysis capabilities based on IoT event data.

This special issue sets out to discuss concerns related to privacy in process analytics over IoT-based event streams. Three interviews with leading experts illustrate the challenges in the field. The reports Process Mining and Privacy in Smart Manufacturing, Process Mining for Learning User Privacy in D2D and IoT Networks*, and* Post-Quantum Cryptography and its Application to the IoT *provide an overview of how some of the challenges encountered could be approached in industry or research settings. Several extended abstracts then outline recent scientific advances on privacy-awareness in process analytics.*

We hope that you will enjoy reading this special issue, and that it will stimulate further work in the field,

Agnes Koschmider, Martin Degeling, Matthias Weidlich

https://doi.org/10.1007/s00287-019-01214-w