SN Computer Science (2020) 1:250
https://doi.org/10.1007/s42979-020-00261-5

EDITORIAL

Topical Issue on Privacy, Data Protection, and Digital Identity

The growing use of digital services is leading to generalized concerns on privacy. Processing of personal data is carried out by all sorts of entities, including, in many cases, third parties. National and/or regional legislation, such as EU's General Data Protection Regulation (GDPR), aims at providing legal assurances in what concerns the protection of personal data/Personal Identifiable Information (PII). On other hand, an increasing number of frameworks, tools, and applications, demand personal data—such as identity-related data, social security data, financial data, and sensitive individual health data—covering all sorts of areas, from public administration to the private sector. Given the above, ways for guaranteeing privacy, for protecting personal data and for ensuring digital identity have never been so highly sought and, in fact, constitute an important challenge of our data-driven society.

In this context, this topical issue attracted original, previously unpublished research, on subject matters that include, but are not restricted to: privacy enhancing architectures, frameworks, mechanisms, tools, and business processes; privacy-enhancing technologies (PETs); technical solutions for supporting GDPR compliance; data protection governance; technical solutions for supporting consent in information society services; data protection by design and/or data protection by default principles; use of blockchain in privacy protection and/or GDPR compliance; privacy-aware identity management; privacy-aware access control; privacy and data protection in cloud-based systems, IoT systems, and smart environments; privacy-related risk assessment and management; and pilots and use cases.

In the paper "Protecting citizens' personal data and privacy: a joint effort from GDPR EU cluster research projects", Renata M. de Carvalho, Camillo Del Prete, Yod Samuel Martin, Rosa M. Araujo Rivero, Melek Onen, Francesco Paolo Schiavo, Angel Cuevas Rumín, Haralambos Mouratidis, Juan C. Yelmo, and Maria N. Koukovini, provide an overview of the work currently being done by a set of European Union projects on the H2020 DS-08-2017 topic, namely BPR4GDPR, DEFeND, SMOOTH, PDP4E, PAPAYA, and PoSeID-on. The aim, scope and solutions being developed by these projects are presented, along with a discussion on the ways in which the projects cooperate and complement each other.

The paper "On Enabling GDPR Compliance in Business Processes Through Data-Driven Solutions", by Rashid Zaman and Marwan Hassani, addresses the problem of data minimization and privacy by design and by default. The paper presents some techniques for the reduction of not necessarily personal data in a processing activity. The proposed techniques explore event-driven data degradation by reducing personal data details, thus minimizing the risk for data subjects, while maintaining processing efficiency. The techniques are explained through various examples.

In the paper "Risk Management and Privacy Violation Detection in the PoSeID-on Data Privacy Platform", by Paulo Silva, Rui Casaleiro, Paulo Simões, Nuno Antunes, Marilia Curado and Edmundo Monteiro, the authors present and discuss a platform that supports personal data transactions between data subjects and private and public organizations that process the data. The platform gives data subjects control over their data and ensures GDPR compliance. The paper focuses on two of the main platform modules, namely Risk Management Module (RMM) and Personal Data Analyzer (PDA). The latter includes functionality for the recognition of personal data, based on semantic and syntactic recognition direct messages, RPC inputs, PDF, TXT, or other types of structured information. The paper presents some experimental results.

The paper "Achieving Privacy Preservation Constraints in Missing-Value Datasets", by Surapon Riyana, Srikul Nanthachumphu, and Noppamas Riyana, is focused on the need for anonymization techniques that, unlike k-Anonymity, l-Diversity, and t-Closeness, are able to effectively cope with datasets where not all attributes are assumed to be complete. The paper proposes an anonymization model, based on k-Anonymity and making use of Correlated Attribute and Tuple Values (CAV/CTV) and Domain Generalization Hierarchies (DGH), that addresses privacy violation issues in missing-value datasets, while achieving a fair degree of data usability.

Finally, in the paper "Privacy Preserving Data Sharing by Integrating Perturbed Distance Matrices", Hanten Chang and Hiroyasu Ando address the issue of inter-organizational data sharing and the privacy implications thereof. To this end, they propose a technique for privacy-preserving data sharing among distributed nodes, allowing collaborative computation without raw data disclosure. The description of the proposed method is complemented by comprehensive experimentation upon sensitive health data that demonstrates the effectiveness of the approach.

As a final remark, the guest editors would like to thank all the reviewers for their effort in putting together this Topical Issue.

The Guest editors
Fernando Boavida, University of Coimbra, Portugal
Andrea Praitano, Maticmind S.p.A, and Hermes University of Rome, Rome, Italy
Georgios V. Lioudakis, ICT abovo P.C., Athens, Greece